Postverlagsort Berlin

MATHEMATISCHE ZEITSCHRIFT.

UNTER STÄNDIGER MITWIRKUNG VON

E. KAMKE
TÜBINGEN

K. KNOPP
TÜBINGEN

R. NEVANLINNA
HELSINKI

E. SCHMIDT
BERLIN

F. K. SCHMIDT
HEIDELBERG

HERAUSGEGEBEN VON

H. WIELANDT
TÜBINGEN

WISSENSCHAFTLICHER BEIRAT

W. BLASCHKE L. FEJÉR A. E. INGHAM
H. KNESER W. MAGNUS O. PERRON W. SÜSS

65. BAND, 1. HEFT

(ABGESCHLOSSEN AM 31. MAI 1956)

QA1
M88
v.65-67

BERLIN · GÖTTINGEN · HEIDELBERG
SPRINGER-VERLAG
1956

Math. Z.

Die **MATHEMATISCHE ZEITSCHRIFT**

wurde im Jahre 1918 von *L. Lichtenstein* unter der Mitwirkung von *K. Knopp*, *E. Schmidt* und *I. Schur* gegründet und herausgegeben. Nach dem Tode Lichtensteins übernahm *K. Knopp* 1933 die Herausgabe. Die Schriftleitung ergänzte sich 1933 durch *E. Kamke* und *F. K. Schmidt*, 1936 durch *R. Nevanlinna* und 1950 durch *H. Wielandt*, der 1952 die Herausgabe übernahm.

Die Zeitschrift erscheint nach Maßgabe des eingehenden Materials. Der Preis des Bandes beträgt DM 96.—.

Die Mathematische Zeitschrift ist durch jede Buchhandlung zu beziehen.

Die Mathematische Zeitschrift dient der Pflege der reinen Mathematik, doch werden auch Beiträge aus den Gebieten der theoretischen Physik und Astronomie Aufnahme finden, soweit sie mathematisch von Interesse sind. Besprechungen, Aufgaben u. dgl. werden nicht zugelassen.

Es wird ausdrücklich darauf aufmerksam gemacht, daß mit der Annahme des Manuskriptes und seiner Veröffentlichung durch den Verlag das ausschließliche Verlagsrecht für alle Sprachen und Länder an den Verlag übergeht, und zwar bis zum 31. Dezember desjenigen Kalenderjahres, das auf das Jahr des Erscheinens folgt. Hieraus ergibt sich, daß grundsätzlich nur Arbeiten angenommen werden können, die vorher weder im Inland noch im Ausland veröffentlicht worden sind, und die auch nachträglich nicht anderweitig zu veröffentlichen der Autor sich verpflichtet.

Die Mitarbeiter erhalten von ihren Arbeiten 75 Sonderdrucke unentgeltlich.

Manuskriptsendungen sind zu richten an die Mitglieder der unterzeichneten Redaktion. Die Herren Mitarbeiter werden im Interesse einer raschen Drucklegung gebeten, die Arbeiten in gut lesbarer Niederschrift einzureichen. Für den Text ist, wenn irgendmöglich, Maschinenschrift, für die mathematischen Formeln jedoch nur Handschrift zu verwenden. Etwaige Abbildungen sind auf einem besonderen Blatt zu zeichnen. Die in den Formeln etwa vorkommenden griechischen oder deutschen Buchstaben (Fraktur) sowie andere der Gefahr von Verwechselungen ausgesetzte Zeichen, z.B. die Landauschen Symbole o und O, sind stets besonders (etwa mit verschiedenfarbigen Stiften) zu kennzeichnen. Die Fußnoten sind fortlaufend zu numerieren, bei Zitaten Erscheinungsjahr und Seitenzahlen anzugeben.

Wenn zu einer bereits gedruckten Arbeit eine Berichtigung nötig wird, wollen die Herren Verfasser dem Herausgeber hiervon unverzüglich Mitteilung machen. Die Berichtigungen sollen dann am Schlusse eines Bandes gesammelt aufgenommen werden.

REDAKTION DER MATHEMATISCHEN ZEITSCHRIFT:

E. Kamke, Tübingen, Frischlinstraße 27,
K. Knopp, Tübingen, Am Apfelberg 6,
R. Nevanlinna, Helsinki (Finnland), Mäntytie 5 B,
E. Schmidt, Berlin-Steglitz, Sedanstraße 8,
F. K. Schmidt, Heidelberg, Mathematisches Institut,
H. Wielandt, Tübingen, Ob dem Viehweidle 21 b.

Springer-Verlag OHG — Berlin W 35 Reichpietschufer 20. — Heidelberg, Neuenheimer Landstraße 24. — Göttingen, Weender Straße 60.

---

65. Band **Inhalt** 1. Heft

Seite

Endl, K., Orthogonalisierung auf einem k-strahligen symmetrischen Integrationsstern 1

Endl, K., Über eine ausgezeichnete Eigenschaft der Koeffizientenmatrizen des Laguerreschen und des Hermiteschen Polynomsystems 7

Schoeneberg, B., Über die Diskriminante der elliptischen Funktionen und ihre Quadratwurzel 16

Dold, A., Erzeugende der Thomschen Algebra $\mathfrak{N}$. 25

Neumann, H., On varieties of groups and their associated near-rings 36

Foster, A. L., Ideals and their Structure in Classes of Operational Algebras 70

Krull, W., Über reelle Radikalkörper 76

Naumann, H., Beliebige konvexe Polytope als Schnitte und Projektionen höherdimensionaler Würfel, Simplizes und Maßpolytope 91

Landsberg, M., Lineare topologische Räume, die nicht lokalkonvex sind 104

ENDL, K.
Math. Zeitschr. Bd. 65, S. 1—6 (1956)

Orthogonalisierung auf einem k-strahligen symmetrischen Integrationsstern

Von
KURT ENDL

Einleitung

Im Laufe einer Untersuchung über LAGUERREsche und HERMITEsche Polynome[1]) stellte sich dem Verfasser folgendes Problem: Gibt es für beliebiges natürliches k einen Orthogonalisierungsprozeß, der Polynome von der Struktur

$$(1) \qquad P_n(z) = p_n^{(n)} \cdot z^n + p_{n-k}^{(n)} \cdot z^{n-k} + p_{n-2k}^{(n)} \cdot z^{n-2k} + \cdots \qquad (p_\nu^{(n)} = 0 \text{ für } \nu < 0)$$

erzeugt? Alle bisher bekannten Orthogonalisierungsverfahren liefern nur Polynome $P_n(z)$ mit $k=1$ (LAGUERRE, JACOBI) und $k=2$ (HERMITE, GEGENBAUER, LEGENDRE, TSCHEBYSCHEFF). *Es wird gezeigt, daß es für jedes natürliche k Orthogonalisierungsverfahren gibt, die Polynome von der Bauart* (1) *erzeugen.* Das wesentliche Kennzeichen jedes dieser Verfahren besteht darin, in bezug auf Orthogonalisierungs-„Intervall" und Belegungsfunktion eine Symmetrie der Ordnung k zu enthalten: Es wird auf einem k-strahligen symmetrischen Stern mit Hilfe einer Belegungsfunktion orthogonalisiert, die invariant gegen solche Drehungen des Sternes ist, die ihn in sich selbst überführen. Zum Schlusse wird bewiesen, daß jedes auf einem k-strahligen Stern orthogonales Polynomsystem $\{P_n(z)\}$ k Teilsysteme $\{P_m^{(\varrho)}(z)\}$ $(\varrho = 0, 1, \ldots, k-1)$ enthält, von denen jedes für sich im klassischen Sinn ein orthogonales Polynomsystem bildet, und daß umgekehrt durch „Ineinanderschachteln" von k geeigneten (im klassischen Sinne orthogonalen) Polynomsystemen, ein neues Polynomsystem erzeugt werden kann, das orthogonal auf einem k-strahligen Stern ist, und dessen Polynome die Struktur (1) besitzen.

§ 1. Der allgemeine Orthogonalisierungsprozeß und die Lückeneigenschaft der zugehörigen orthogonalen Polynome

Die Ursache dafür, daß bei Orthogonalisierung der Potenzen x^n auf einem Intervall $[a, b]$ mit einer Belegungsfunktion $p(x)$ Polynome von der Struktur (1) mit $k=2$ auftreten (also abwechselnd gerade und ungerade Polynome) liegt darin, daß die Belegungsfunktion $p(x)$ in bezug auf das Orthogonalisierungsintervall $[a, b]$ eine Symmetrieeigenschaft besitzt[2]). Diese einfache

[1]) ENDL, KURT: Sur une classe de polynômes orthogonaux généralisant ceux de Laguerre et Hermite. C. R. Acad. Sci. **241**, 723—724 (1955) und ENDL, KURT: Über eine ausgezeichnete Eigenschaft der Koeffizientenmatrizen des LAGUERREschen und des HERMITEschen Polynomsystems. Math. Z. **65**, 7—15 (1956).

[2]) Dies folgt durch eine einfache Überlegung aus dem ERHARD-SCHMIDTschen Orthogonalisierungsverfahren.

Bemerkung läßt vermuten, daß ein Orthogonalisierungsprozeß, der für beliebiges natürliches k Polynome von der Form (1) erzeugen soll, eine Symmetrie in bezug auf Belegungsfunktion und Orthogonalisierungs-„Intervall" besitzen muß, wobei diese Symmetrie noch in irgendeiner Form den Parameter k enthalten muß. Wir betrachten dazu in der komplexen z-Ebene k Strecken $\mathfrak{S}_\lambda$ in symmetrischer Anordnung (k fest, $\lambda = 0, 1, \ldots, k-1$), die im 0-Punkt zusammenlaufen; es sei z.B. $\mathfrak{S}_\lambda = \mathfrak{S}_\lambda^{(R,k)}$ die Menge der Punkte $z = r \cdot e^{\frac{2\pi i}{k}\lambda}$ $(0 \leq r \leq R)$. Diese k Strecken $\mathfrak{S}_\lambda$ bilden eine Punktmenge, die wir einen k-strahligen symmetrischen Stern nennen und mit $\mathfrak{S} = \mathfrak{S}_R^{(k)}$ bezeichnen. Ferner wählen wir eine Belegungsfunktion $p(z)$, die invariant gegen Drehungen um $\frac{2\pi}{k}$ ist, für die also gilt $p(z) = p\left(z \cdot e^{\frac{2\pi i}{k}}\right)$. Definieren wir nun als skalares Produkt

$$(2) \qquad (P, Q)_{p(z)}^{(k)} = (P, Q) = \int_{\mathfrak{S}} P \overline{Q}\, p\, dr = \sum_{\lambda=0}^{k-1} \int_0^R P(z)\, \overline{Q(z)}\, p(z)\, dr,$$

so liegt offenbar ein Orthogonalisierungsprozeß vor, der in bezug auf Belegungsfunktion und „Orthogonalisierungsintervall" eine Symmetrieeigenschaft besitzt. Durch Orthogonalisierung der Potenzen $\{z^n\}$ mit Hilfe des skalaren Produktes (2) entsteht nun ein orthogonales Polynomsystem

$$P_n(z) = p_n^{(n)} \cdot z^n + p_{n-1}^{(n)} z^{n-1} + \cdots + p_0,$$

das wir uns gleich so normiert denken, daß $p_n^{(n)} = 1$ ist $(n = 0, 1, \ldots)$. Wir behaupten folgenden

Satz I. *Alle Polynome $P_n(z)$ besitzen die Struktur* (1)

$$P_n(z) = 1 \cdot z^n + p_{n-k}^{(n)} \cdot z^{n-k} + p_{n-2k}^{(n)} \cdot z^{n-2k} + \cdots,$$

d.h. $p_\nu^{(n)} = 0$ für $\nu \not\equiv n \,(k)$ $(0 \leq \nu \leq n = 0, 1, \ldots)$. Nimmt weiterhin die Belegungsfunktion $p(z)$ auf einem Strahl $\mathfrak{S}_\lambda$ nur reelle Werte an, so sind die Polynome $P_n(z)$ reell $(n = 0, 1, \ldots)$.

Beweis. $P_0(z) \equiv p_0^{(0)} = 1$ hat trivialerweise die Form (1). Wir nehmen an, dies sei auch für alle $P_\nu(z)$ mit $0 \leq \nu < n$ erfüllt, d.h.

$$P_\nu(z) = z^\nu + p_{\nu-k}^{(\nu)} z^{\nu-k} + \cdots \qquad (p_\mu^{(\nu)} = 0 \quad \text{für } \mu < 0)$$

oder wenn wir alle natürlichen Zahlen n in der Form zerlegen $n = n_k^* + n_k \cdot k$ $(0 \leq n_k^* < k)$

$$(3) \qquad P_\nu(z) = \sum_{\varkappa=0}^{\nu_k} p_{\nu_k^* + \varkappa k}^{(\nu)} \cdot z^{\nu_k^* + \varkappa k}.$$

Nach ERHARD SCHMIDT erhält man für $P_n(z)$ die Beziehung

$$(4) \qquad P_n(z) = z^n - \sum_{\nu=0}^{n-1} C_\nu P_\nu(z),$$

wobei $C_\nu = \frac{(z^n, P_\nu)}{(P_\nu, P_\nu)}$ ist.

Für $(z^n, P_\nu(z))$ folgt aus (3)

$$(z^n, P_\nu) = \sum_{\lambda=0}^{k-1} \int_{\mathfrak{S}_\lambda}^{R} z^n \overline{P_\nu(z)}\, p(r)\, dr$$

$$= \sum_{\varkappa=0}^{\nu_k} \overline{p_{\nu_k^*+\varkappa k}^{(\nu)}} \cdot \left\{ \sum_{\lambda=0}^{k-1} \int_{\mathfrak{S}_\lambda}^{R} z^n \cdot \overline{z^{\nu_k^*+\varkappa k}} \cdot p(r)\, dr \right\}$$

$$= \sum_{\varkappa=0}^{\nu_k} \overline{p_{\nu_k^*+\varkappa k}^{(\nu)}} \cdot \int_0^R r^{n+\nu_k^*+\varkappa k} \left\{ \sum_{\lambda=0}^{k-1} \left[e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)} \right]^\lambda \right\} p(r)\, dr.$$

Ist $\nu \equiv n(k)$, d.h. $\nu_k^* = n_k^*$, so ist $n - \nu_k^* - \varkappa k = (n_k - \varkappa) \cdot k \equiv o(k)$ d.h.

$$\sum_{\lambda=0}^{k-1} \left[e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)} \right]^\lambda = \sum_{\lambda=0}^{k-1} 1 = k$$

und damit

$$(z^n, P_\nu) = k \cdot \sum_{\varkappa=0}^{\nu_k} \overline{p_{\nu_k^*+\varkappa k}^{(\nu)}} \cdot \int_0^R r^{n+\nu_k^*+\varkappa k}\, p(r)\, dr.$$

Dagegen gilt für $\nu \not\equiv n(k)$ wegen $e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)} \neq 1$

$$\sum_{\lambda=0}^{k-1} \left[e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)} \right]^\lambda = \frac{e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)\,k} - 1}{e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)} - 1} = 0$$

und damit $(z^n, P_\nu) = 0$.

In der Entwicklung (4) treten also nur Koeffizienten C_ν mit $\nu \equiv n(k)$ auf. Wir können schreiben:

$$P_n(z) = z^n - \sum_{\nu=0}^{n_k-1} C_{n_k^*+\nu k} \cdot P_{n_k^*+\nu k}(z)$$

$$= z^n - \sum_{\nu=0}^{n_k-1} C_{n_k^*+\nu k} \cdot \sum_{\varkappa=0}^{\nu} p_{n_k^*+\varkappa k}^{(n_k^*+\nu k)} \cdot z^{n_k^*+\varkappa k},$$

woraus nach Vertauschung der Summationen folgt:

$$(5) \qquad P_n(z) = z^n - \sum_{\varkappa=0}^{n_k-1} z^{n_k^*+\varkappa k} \cdot \left\{ \sum_{\nu=\varkappa}^{n_k-1} C_{n_k^*+\nu k} \cdot p_{n_k^*+\varkappa k}^{(n_k^*+\nu k)} \right\}.$$

Hiermit ist der erste Teil des Satzes I bewiesen. Um den zweiten Teil nachzuprüfen, sei als Induktionsannahme noch hinzugenommen, daß alle Polynome $P_\nu(z)$ reelle Polynome sind. Dann sind, da $\int_0^R r^{n+\nu_k^*+\varkappa k} p(r)\, dr$ reell ist, C_ν und damit alle Koeffizienten in (5) reell.

§ 2. Die orthogonalen Untersysteme des Systemes $\{P_n(z)\}$

Wie an anderer Stelle gezeigt wurde[3]), läßt sich mit Hilfe des in § 1 wiedergegebenen Orthogonalisierungsverfahrens [man setzt in (2) $R=\infty$ und $p(z)=e^{-z^k}$] ein mit einem natürlichen Parameter k versehenes Polynomsystem $\{P_{k,n}(z)\}$ erzeugen, das als Spezialfälle die LAGUERREschen Polynome $\{L_n(z)\}$ und HERMITEschen Polynome $\{H_n(z)\}$ umfaßt. Es gilt $\{P_{1,n}\}=\{L_n\}$ und $\{P_{2,n}\}=\{H_n\}$. Die Polynome $P_{k,n}(z)$ lauten explizit

$$P_{k,n}(z)=n_k!\sum_{\nu=0}^{n_k}\frac{(-)^{n_k-\nu}}{\nu!}\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k-\nu}z^{n_k^*+\nu k}.$$

Vergleicht man diesen Ausdruck mit dem der verallgemeinerten LAGUERREschen Polynome

$$L_n^{(\alpha)}(z)=n!\sum_{\nu=0}^{n}(-)^{n-\nu}\binom{n+\alpha}{n-\nu}\frac{z^\nu}{\nu!},$$

so bemerkt man eine gewisse Verwandtschaft. In der Tat lassen sich die Polynome $P_{k,n}(z)$ durch die Polynome $L_n^{(\alpha)}(z)$ folgendermaßen ausdrücken:

$$P_{k,n}(z)=z^{n_k^*}\cdot L_{n_k}^{\left(\frac{2n_k^*+1}{k}-1\right)}(z^k).$$

Der Rest n_k^* geht hierbei in den Parameterwert α ein, das Vielfache n_k in den Grad des LAGUERREschen Polynomes. Betrachten wir für den Augenblick die Unterklasse der Polynome $P_{k,n}(z)$ mit demselben Rest ϱ $(0, 1, \ldots, k-1)$, d.h. die Polynome $\{P_{k,\varrho+mk}(z)\}$ $(m=0, 1, \ldots)$, so finden wir: Das Untersystem $\{P_{k,\varrho+mk}(z)\}$ ist bis auf Multiplikation mit der Potenz z^ϱ und bis auf die Substitution $z^k=\zeta$ ein im klassischen Sinn orthogonales Polynomsystem. Es ist nämlich orthogonal auf dem Intervall $[0, \infty]$ mit der Belegungsfunktion $\zeta^{\frac{2\varrho+1}{k}-1}e^{-\zeta}$. Da dies für $\varrho=0, 1, \ldots, k-1$ gilt, folgt die Aussage: Das System $\{P_{k,n}(z)\}$ ist aus k im klassischen Sinn orthogonalen Polynomsystemen zusammensetzt.

Dieser Sachverhalt, den wir in diesem Spezialfall bemerkt haben, ist allgemein richtig[4]). Jedes auf einem k-strahligen Stern orthogonale Polynomsystem entsteht durch Ineinanderschachtelung von k (im klassischen Sinn orthogonalen) Polynomsystemen; umgekehrt kann man k geeignete (klassische) Systeme zu einem neuen System zusammensetzen. Um dies zu präzisieren,

---

[3]) ENDL, KURT: Les polynomes de Laguerre et de Hermite comme cas particuliers d'une classe de polynomes orthogonaux. Ann. Ec. Norm. (3), **73**, fasc. 1, 1—13 (1956).

[4]) Der Verfasser glaubte ursprünglich, daß es sich um eine besondere Eigentümlichkeit des Systems $P_{k,n}(z)$ handele, bedingt durch die Belegungsfunktion e^{-z^k}. Daß dieser Sachverhalt allgemein zutreffend ist, geht auf eine Diskussionsbemerkung von H. WOLFGANG HAHN im Anschluß an den Vortrag des Verfassers auf der DMV-Tagung 1955 in Göttingen zurück.

betrachten wir das auf dem k-strahligen Stern $\mathfrak{S}$ mit der Belegungsfunktion $p(z)$ orthogonale Polynomsystem

$$P_n(z) = \sum_{\nu=0}^{n} p_\nu^{(n)} z^\nu.$$

Nach § 1 können wir $P_n(z)$ in der Form schreiben:

$$P_n(z) = P_{n_k^* + n_k \cdot k}(z) = \sum_{\nu=0}^{n_k} p_{n_k^* + \nu k}^{(n)} z^{n_k^* + \nu k} = z^{n_k^*} \cdot \sum_{\nu=0}^{n_k} p_{n_k^* + \nu k}^{(n)} (z^k)^\nu.$$

Wir betrachten nun alle Polynome $P_n(z)$ in derselben Restklasse ϱ ($\varrho = 0, 1, \ldots, k-1$)

$$P_{\varrho + m k}(z) = z^\varrho \sum_{\nu=0}^{m} p_{\varrho+\nu k}^{(\varrho + m k)} (z^k)^\nu \qquad (\varrho \text{ fest}, \; m = 0, 1, \ldots).$$

Diese Polynome bilden ein Untersystem des Gesamtsystems $\{P_n(z)\}$. Wenn wir von der multiplikativen Potenz z^ϱ absehen und $z^k = \zeta$ setzen, ist dieses Untersystem ein vollständiges Polynomsystem im gewöhnlichen Sinn, d.h. es enthält Polynome aller Grade m. Wir bezeichnen die Polynome des so erhaltenen ϱ-ten Polynomsystems mit

$$P_m^{(\varrho)}(\zeta) = \sum_{\nu=0}^{m} p_{\varrho+\nu k}^{(\varrho + m k)} \zeta^\nu$$

und behaupten

Satz II. A. *Jedes der Systeme $\{P_m^{(\varrho)}(\zeta)\}$ ist schon für sich ein im klassischen Sinn orthogonales Polynomsystem. Es ist orthogonal auf dem Intervall $[0, R^k]$ mit der Belegungsfunktion $p_\varrho(\zeta) = \zeta^{\frac{2\varrho+1}{k} - 1} \cdot p\left(\zeta^{\frac{1}{k}}\right)$:*

$$(P_n^{(\varrho)}, P_m^{(\varrho)})_\varrho = \int_0^{R^k} P_n^{(\varrho)}(\zeta) \, \overline{P_m^{(\varrho)}(\zeta)} \, p_\varrho(\zeta) \, d\zeta = 0 \qquad \text{für } n \neq m.$$

Hierzu gilt die folgende Umkehrung:

B. *Ist k eine beliebige natürliche Zahl, $p(\zeta)$ eine beliebige Belegungsfunktion auf dem Intervall $[0, R^k]$, und bezeichnen wir mit $\{P_m^{(\varrho)}(\zeta)\}$ das zu $[0, R^k]$ und der Belegungsfunktion $p_\varrho(\zeta) = \zeta^{\frac{2\varrho+1}{k} - 1} p(\zeta)$ gehörige Polynomsystem*[5] *($\varrho = 0, 1, \ldots, k-1$), so lassen sich diese k Polynomsysteme durch die Festsetzung*

$$P_n(z) = z^{n_k^*} P_{n_k}^{(n_k^*)}(z^k)$$

zu einem neuen Polynomsystem $\{P_n(z)\}$ zusammensetzen. Dieses neue System $\{P_n(z)\}$ ist orthogonal auf dem k-strahligen Stern $\mathfrak{S}$ mit der Belegungsfunktion $p(z^k)$.

---

[5]) Falls die Belegungsfunktion $p(\zeta)$ nicht reell ist, muß hierbei das skalare Produkt lauten:

$$(P, Q)_\varrho = \int P(\zeta) \, \overline{Q(\zeta)} \, p_\varrho(\zeta) \, d\zeta.$$

Wir beginnen mit dem Beweis des Teiles A. Wegen der Orthogonalität der Polynome $P_n(z)$ auf $\mathfrak{S}$ gilt:

$$(6)\quad \left(z^\varrho P_n^{(\varrho)}(z^k), z^\varrho P_m^{(\varrho)}(z^k)\right)^{(k)}_{p(z)} = \sum_{\lambda=0}^{k-1} \int_{\mathfrak{S}_\lambda}^{R} z^\varrho P_n^{(\varrho)}(z^k) \cdot \overline{z^\varrho P_n^{(\varrho)}(z^k)}\, p(z)\, dr = 0 \quad \text{für } m \neq n.$$

Dieses skalare Produkt formen wir um

$$\sum_{\lambda=0}^{k-1} \int_{\mathfrak{S}_\lambda}^{R} z^\varrho P_n^{(\varrho)}(z^k) \overline{z^\varrho P_m^{(\varrho)}(z^k)}\, p(r)\, dr -$$

$$= \sum_{\nu=0}^{n} \sum_{\mu=0}^{m} p_{\varrho+\nu k}^{(\varrho+n k)} \cdot \overline{p_{\varrho+\mu k}^{(\varrho+m k)}} \int_0^R r^{2\varrho+\nu k+\mu k} \left\{ \sum_{\lambda=0}^{k-1} \left[e^{\frac{2\pi i}{k}(\varrho+\nu k-\varrho-\mu k)} \right]^\lambda \right\} p(r)\, dr$$

$$= k \int_0^R \left(\sum_{\nu=0}^{n} p_{\varrho+\nu k}^{(\varrho+n k)} (r^k)^\nu \right) \left(\sum_{\mu=0}^{m} p_{\varrho+\mu k}^{(\varrho+m k)} (r^k)^\mu \right) r^{2\varrho}\, p(r)\, dr$$

$$= k \int_0^R P_n^{(\varrho)}(r^k) \cdot P_m^{(\varrho)}(r^k)\, r^{2\varrho}\, p(r)\, dr.$$

Die Substitution $r^k = \zeta$ liefert weiter

$$= \int_0^{R^k} P_n^{(\varrho)}(\zeta)\, P_m^{(\varrho)}(\zeta)\, \zeta^{\frac{2\varrho+1}{k}-1} p\left(\zeta^{\frac{1}{k}}\right) d\zeta,$$

woraus nach (6) für $m \neq n$ folgt

$$(P_n^{(\varrho)}, P_m^{(\varrho)})_\varrho = 0 \qquad \text{w. z. b. w.}$$

Zum Beweis von B hat man nur die eben durchgeführten Überlegungen rückwärts zu verfolgen.

Gießen, Mathematisches Institut der Universität

(Eingegangen am 9. September 1955)

ENDL, K.
Math. Zeitschr. Bd. 65, S. 7—15 (1956)

Über eine ausgezeichnete Eigenschaft der Koeffizientenmatrizen des Laguerreschen und des Hermiteschen Polynomsystems

Von

KURT ENDL

§ 1. Einleitung

Bei Untersuchungen über Zusammenhänge zwischen LAGUERREschen und HERMITEschen Polynomen[1]) bemerkte der Verfasser eine eigenartige Eigenschaft der LAGUERREschen Polynome[2])

$$L_n(x) = n! \sum_{\nu=0}^{n} \frac{(-)^{n-\nu}}{\nu!} \binom{n}{\nu} x^\nu.$$

Diese Polynome lassen sich so normieren, d.h. jedes Polynom $L_n(x)$ läßt sich so mit einem Faktor c_n versehen, daß die zu dem neuen System $L_n^* = c_n L_n$ gehörige Koeffizientenmatrix $\mathfrak{L}^*$ der Matrizengleichung

(1) $\qquad \mathfrak{L}^* = (\mathfrak{L}^*)^{-1} \quad$ oder $\quad (\mathfrak{L}^*)^2 = \mathfrak{E} \qquad$ ($\mathfrak{E}$ Einheitsmatrix)

genügt. Dies kann sogar auf zwei Arten geschehen. In einer dieser ausgezeichneten Normierungen lauten die LAGUERREschen Polynome:

$$L_n^*(x) = n! \sum_{\nu=0}^{n} \frac{(-)^\nu}{\nu!} \binom{n}{\nu} x^\nu.$$

Die Beziehung (1) ist gleichbedeutend mit der Tatsache, daß die Entwicklung der Potenz x^n nach den LAGUERREschen Polynomen $L_\nu^*(x)$ $(0 \leqq \nu \leqq n)$ dieselben Koeffizienten besitzt wie das Polynom $L_n^*(x)$ selbst:

$$x^n = n! \sum_{\nu=0}^{n} \frac{(-)^\nu}{\nu!} \binom{n}{\nu} L_\nu^*(x).$$

---

[1]) ENDL, KURT: Sur les systèmes de polynômes orthogonaux en involution. C. R. Acad. Sci. **241**, 682—684 (1955).

[2]) Für die gesamte Arbeit vgl. z.B. MAGNUS-OBERHETTINGER, Formeln und Sätze für die speziellen Funktionen der mathematischen Physik. Wir normieren jedes orthogonale Polynomsystem $\{P_n(x)\}$ in der Form:

$$\{P_n(x)\} = \left\{ \sum_{\nu=0}^{n} p_\nu^{(n)} x^\nu \right\} = \left\{ x^n + \sum_{\nu=0}^{n-1} p_\nu^{(n)} x^\nu \right\} (n = 0, 1, \ldots).$$

Diese einfache Bemerkung wirft das folgende Problem auf: Handelt es sich hier um eine bisher unbemerkte allgemeine Eigenschaft orthogonaler Polynomsysteme, d.h. kann man jedes orthogonale Polynomsystem

$$\{P_n(x)\} = \left\{ \sum_{\nu=0}^{n} p_\nu^{(n)} x^\nu \right\} \qquad (p_n^{(n)} = 1)$$

mit einer solchen Normierung $\{c_n\}$ versehen, daß die zu dem neuen System $\{P_n^*(x)\} = \{c_n P_n(x)\}$ gehörige Koeffizientenmatrix $\mathfrak{P}^* = (c_n p_\nu^{(n)})$ der zu (1) analogen Beziehung genügt:

$$\mathfrak{P}^* = (\mathfrak{P}^*)^{-1} \quad \text{oder} \quad (\mathfrak{P}^*)^2 = \mathfrak{E}. \tag{2}$$

Dies ist nun nicht der Fall. Nennen wir ein orthogonales Polynomsystem $\{P_n(x)\}$, für das eine solche Normierung gefunden werden kann, kurz ein involutorisches Polynomsystem, und das System $\{P_n^*(x)\} = \{c_n P_n(x)\}$, für dessen Matrix $\mathfrak{P}^*$ (2) erfüllt ist, eine involutorische Form des Systems $\{P_n(x)\}$, so gilt:

Das LAGUERREsche *System* $\{L_n^{(\alpha)}(x)\}$ *und das* HERMITEsche *System* $\{H_n(x)\}$ *sind unter den klassischen orthogonalen Polynomsystemen die einzigen involutorischen Systeme.*

Dieses Ergebnis, das auf eine außerordentliche strukturelle Verwandtschaft der LAGUERREschen und HERMITEschen Polynome hinweist, war der Anlaß zu der folgenden Fragestellung: Kann man aus dieser Verwandtschaft der beiden Systeme $\{L_n\}$ und $\{H_n\}$ nicht schon auf die Existenz eines allgemeineren übergeordneten orthogonalen Polynomsystems schließen, das die Systeme $\{L_n\}$ und $\{H_n\}$ als Spezialfälle enthält. Der Verfasser hat mit Hilfe eines von ihm eingeführten neuen Orthogonalisierungsverfahrens[3]) ein von einem ganzzahligen Parameter k ($k = 1, 2, 3, \ldots$) abhängiges orthogonales Polynomsystem $\{P_{k,n}(x)\}$ konstruiert, das für spezielle Parameterwerte das LAGUERREsche und HERMITEsche Polynomsystem enthält[4]). Es gilt:

$$\{P_{1,n}(x)\} = \{L_n(x)\}, \qquad \{P_{2,n}(x)\} = \{H_n(x)\}.$$

Dies sei in diesem Zusammenhang deswegen erwähnt, weil auch für alle $k > 2$ das System $\{P_{k,n}(x)\}$ involutorisch ist.

§ 2. Notwendige und hinreichende Bedingungen für die involutorische Eigenschaft eines orthogonalen Polynomsystems

Wir betrachten ein beliebiges orthogonales Polynomsystem.

$$\{P_n(x)\} = \left\{ \sum_{\nu=0}^{n} p_\nu^{(n)} x^\nu \right\} \qquad (p_n^{(n)} = 1;\ n = 0, 1, \ldots)$$

[3]) ENDL, KURT: Orthogonalisierung auf einem k-strahligen symmetrischen Integrationsstern. Math. Z. **65**, 1—6 (1956).

[4]) ENDL, KURT: Les Polynomes de Laguerre et de Hermite comme cas particuliers d'une classe de polynomes orthogonaux. Ann. Ec. Norm. (3), **73**, fasc. 1, 1—13 (1956) und ENDL, KURT: Sur une classe de polynomes orthogonaux généralisant ceux de Laguerre et Hermite. C. R. Acad. Sci. **241**, 723—724 (1955).

und bezeichnen wie üblich mit (P_m, P_n) das skalare Produkt, mit dessen Hilfe man durch Orthogonalisation der Potenzen z^n das System $\{P_n(x)\}$ erhält. Zu jedem solchen System gehört eine unendliche Dreiecksmatrix, die Koeffizientenmatrix $\mathfrak{P} = (p_\nu^{(n)})$. Ebenso betrachten wir die inversen Formeln, d.h. die Entwicklungen der Potenzen x^n nach den Polynomen $\{P_n\}$

$$x^n = \sum_{\nu=0}^{n} q_\nu^{(n)} P_\nu(x).$$

Diese Entwicklungen liefern uns eine neue Matrix $(q_\nu^{(n)})$, die wir mit $\mathfrak{P}^{-1}$ bezeichnen; denn es gilt:

$$(q_\nu^{(n)})\,(p_\nu^{(n)}) = (p_\nu^{(n)})\,(q_\nu^{(n)}) = \mathfrak{E} \qquad (\mathfrak{E} \text{ Einheitsmatrix}).$$

Die Frage, welche Polynomsysteme $\{P_n(x)\}$ involutorisch sind, ist gleichbedeutend mit der folgenden: Für welche Systeme $\{P_n(x)\}$ kann man Koeffizienten $c_n \neq 0$ $(n = 0, 1, \ldots)$ so finden, daß für die Polynome

$$P_n^*(x) = c_n \cdot P_n(x) = \sum_{\nu=0}^{n} c_n p_\nu^{(n)} x^\nu = \sum_{\nu=0}^{n} p_\nu^{*(n)} x^\nu$$

gilt:

$$x^n = \sum_{\nu=0}^{n} p_\nu^{*(n)} P_\nu^*(x) \qquad (n = 0, 1, 2, \ldots). \tag{3}$$

Nehmen wir an, für $\{P_n(x)\}$ seien Koeffizienten c_n gefunden die (3) erfüllen. Da die Koeffizienten $a_\nu^{(n)}$ in der Entwicklung

$$x^n = \sum_{\nu=0}^{n} a_\nu^{(n)} P_\nu^*(x)$$

bekanntlich lauten:

$$a_\nu^{(n)} = \frac{(x^n, P_\nu^*)}{(P_\nu^*, P_\nu^*)} = \frac{1}{c_\nu} \cdot \frac{(x^n, P_\nu)}{(P_\nu, P_\nu)} \qquad 0 \leq \nu \leq n,$$

folgt aus (3) die Aussage:

$$a_\nu^{(n)} = p_\nu^{*(n)} = c_n \cdot p_\nu^{(n)} = \frac{1}{c_\nu} \cdot \frac{(x^n, P_\nu)}{(P_\nu, P_\nu)} \qquad 0 \leq \nu \leq n = 0, 1, \ldots$$

oder

$$c_n \cdot c_\nu \cdot p_\nu^{(n)} = \frac{(x^n, P_\nu)}{(P_\nu, P_\nu)} \qquad 0 \leq \nu \leq n = 0, 1, \ldots. \tag{4}$$

Ist umgekehrt (4) erfüllt, so folgt (3). Setzen wir in (4) noch $\nu = n$, so erhalten wir wegen $p_n^{(n)} = 1$ und der Beziehung

$$\left(\sum_{\nu=0}^{n-1} p_\nu^{(n)} x^\nu, P_n\right) = 0$$

$$c_n^2 = \frac{(x^n, P_n)}{(P_n, P_n)} = \frac{\left(x^n + \sum_{\nu=0}^{n-1} p_\nu^{(n)} x^\nu, P_n\right)}{(P_n, P_n)} = \frac{(P_n, P_n)}{(P_n, P_n)} = 1,$$

d.h. $c_n = \pm 1$ $(n = 0, 1, \ldots)$. Damit gilt der

Satz I. *Das orthogonale Polynomsystem* $\{P_n(x)\} = \left\{\sum_{\nu=0}^{n} p_\nu^{(n)} x^\nu\right\}$ $(p_n^{(n)} = 1)$ *ist genau dann involutorisch, wenn sich ein Vorzeichensystem* $\{c_n\}$ *so finden läßt, daß für alle Wertepaare* (n, ν) *mit* $0 \leqq \nu \leqq n = 0, 1, \ldots$ *die Beziehung erfüllt ist:*

$$c_n \cdot c_\nu \cdot p_\nu^{(n)} = \frac{(x^n, P_\nu)}{(P_\nu, P_\nu)}. \tag{5}$$

Nützlich für die Anwendung in Einzelfällen ist das folgende *Korollar:* Das orthogonale Polynomsystem $\{P_n(x)\}$ ist bestimmt nicht involutorisch, wenn auch nur für ein Wertepaar (n, ν) $|p_\nu^{(n)}| \neq \left|\frac{(x^n, P_\nu)}{(P_\nu, P_\nu)}\right|$ ist.

§ 3. Behandlung der klassischen Polynomsysteme

Beginnen wir mit den LAGUERREschen Polynomen

$$L_n^{(\alpha)}(x) = n! \sum_{\nu=0}^{n} \frac{(-)^{n-\nu}}{\nu!} \binom{n+\alpha}{n-\nu} x^\nu.$$

Man berechnet leicht:

$$(x^n, L_\nu^{(\alpha)}) = \int_0^\infty x^n L_\nu^{(\alpha)} x^\alpha e^{-x}\, dx$$

$$= \Gamma(n + \alpha + 1) \cdot \nu! \binom{n}{\nu}.$$

Da $(L_\nu^{(\alpha)}, L_\nu^{(\alpha)}) = \Gamma(1+\alpha)\,(\nu!)^2 \binom{\nu+\alpha}{\nu}$ ist, ergibt (5):

$$c_n \cdot c_\nu = (-)^n\,(-)^\nu.$$

Diese Gleichung erlaubt zwei Lösungssysteme $\{c_n^{(1)}\} = \{(-)^n\}$ und $\{c_n^{(1)}\} = \{(-)^{n+1}\}$. Daher folgt:

Das LAGUERREsche *System ist involutorisch. Es besitzt genau zwei involutorische Formen.*

Das System $L_n^*(x)$ von § 1 erhält man offenbar für $\{c_n^{(1)}\} = \{(-)^n\}$ und $\alpha = 0$. Allgemein gilt mit den Vorzeichen $\{c_n^{(1)}\}$

$$L_n^{*(\alpha)}(x) = n! \sum_{\nu=0}^{n} \frac{(-)^\nu}{\nu!} \binom{n+\alpha}{n-\nu} x^\nu$$

und daher:

$$x^n = n! \sum_{\nu=0}^{n} \frac{(-)^\nu}{\nu!} \binom{n+\alpha}{n-\nu} L_\nu^{*(\alpha)}(x).$$

Zur Behandlung der HERMITEschen Polynome

$$H_n(x) = \frac{1}{2^n} \sum_{\nu=0}^{[n/2]} (-)^\nu \binom{n}{2\nu} \frac{(2\nu)!}{\nu!} (2x)^{n-2\nu}$$

ersetzen wir in (5) ν durch $n-2\nu$. Da durch eine ähnliche Rechnung wie für die LAGUERREschen Polynome folgt:

$$(x^n, H_{n-2\nu}) = \int_{-\infty}^{+\infty} x^n H_{n-2\nu}\, e^{-x^2}\, dx = \frac{1}{2^n} \cdot \frac{n!}{\nu!} \sqrt{\pi}$$

und da $(H_{n-2\nu}, H_{n-2\nu}) = \frac{(n-2\nu)!}{2^{n-2\nu}} \cdot \sqrt{\pi}$ ist, folgt aus (5) als Bestimmungsgleichung für die Vorzeichen c_n:

$$c_n \cdot c_{n-2\nu} = (-)^\nu \qquad 0 \leq \nu \leq \left[\frac{n}{2}\right];\ n = 0, 1, 2, \ldots .$$

Setzen wir hier $\nu = [n/2]$, so ergibt sich für $n = 2m$: $c_{2m} = (-)^m c_0$ für $n = 2m+1$: $c_{2m+1} = (-)^m c_1$. Es können also c_0 und c_1 frei gewählt werden. Wir erhalten vier Vorzeichensysteme:

	c_0	c_1	c_2	c_3	c_4	c_5	c_6	c_7	...
$\{c_n^{(1)}\}$	+	+	−	−	+	+	−	−	...
$\{c_n^{(2)}\}$	+	−	−	+	+	−	−	+	...
$\{c_n^{(3)}\}$	−	+	+	−	−	+	+	−	...
$\{c_n^{(4)}\}$	−	−	+	+	−	−	+	+	... .

Es gilt also: *Das* HERMITE*sche System ist involutorisch. Es besitzt genau vier involutorische Formen.*

Die Vorzeichen $\{c_n^{(1)}\}$ werden durch $\{(-)^{[n/2]}\}$ gegeben. Die zugehörige involutorische Form der HERMITEschen Polynome lautet:

$$H_n^*(x) = (-)^{[n/2]} \sum_{\nu=0}^{[n/2]} \frac{(-)^\nu}{4^\nu} \binom{n}{2\nu} \frac{(2\nu)!}{\nu!}\, x^{n-2\nu}$$

und daher gilt

$$x^n = (-)^{[n/2]} \sum_{\nu=0}^{[n/2]} \frac{(-)^\nu}{4^\nu} \binom{n}{2\nu} \frac{(2\nu)!}{\nu!}\, H_{n-2\nu}^*(x).$$

Um zu beweisen, daß die TSCHEBYSCHEFF*schen Polynome*

$$T_0(x) = 1, \qquad T_n(x) = \frac{\cos(n \cdot \arccos x)}{2^{n-1}} \qquad n \geq 1$$

kein involutorisches Polynomsystem bilden, benutzen wir das Korollar von Satz I, indem wir zeigen, daß für das Wertepaar (4, 0) die beiden Seiten in (5) verschiedenen Betrag haben. Das vierte TSCHEBYSCHEFFsche Polynom lautet: $T_4 = x^4 - x^2 + \frac{1}{8}$. Da

$$(x^4, T_0) = \int_{-1}^{+1} \frac{x^4\, T_0}{\sqrt{1-x^2}}\, dx = \frac{3}{8}\pi, \qquad (T_0, T_0) = \pi$$

ist, folgt:

$$\frac{1}{8} = \left| p_0^{(4)} \right| \neq \frac{(x^4, T_0)}{(T_0, T_0)} = \frac{3}{8}.$$

Ähnlich schließen wir im Fall der LEGENDRE*schen Polynome*

$$P_n(x) = \frac{1}{\binom{2n}{n}} \sum_{\nu=0}^{[n/2]} (-)^\nu \binom{2n-2\nu}{n} \binom{n}{\nu} x^{n-2\nu}.$$

Das vierte Polynom lautet: $P_4 = x^4 - \frac{6}{7}x^2 + \frac{3}{35}$. Für (x^4, P_0) ergibt sich:

$$(x^4, P_0) = \int_{-1}^{+1} x^4 P_0 \, dx = \int_{-1}^{+1} x^4 \, dx = \tfrac{2}{5}.$$

Da $(P_0, P_0) = 2$ ist, folgt

$$\frac{3}{35} = |p_0^{(4)}| \neq \frac{(x^4, P_0)}{(P_0, P_0)} = \frac{1}{5},$$

d.h. auch die LEGENDREschen Polynome bilden kein involutorisches Polynomsystem. Hieraus können wir sofort schließen, daß auch die GEGENBAUERschen Polynome $C_n^{(\nu)}(x)$ für allgemeinen Parameterwert ν nicht involutorisch sind. Denn wäre dies der Fall, so insbesondere auch für $\nu = \frac{1}{2}$. $C_n^{(\frac{1}{2})}$ sind aber gerade die LEGENDREschen Polynome, für die wir oben das Gegenteil bewiesen haben.

Auch die JACOBI*schen Polynome*

$$\mathfrak{F}_n(\alpha, \gamma; x) = (-)^n \frac{\gamma \cdot \overline{\gamma+1} \dots \overline{\gamma+n-1}}{\overline{\alpha+n} \dots \overline{\alpha+2n-1}} F(-n, \alpha+n, \gamma; x)$$

bilden für allgemeine Parameterwerte α und β kein involutorisches System. Denn wählen wir etwa $\alpha = \gamma = 1$, so gilt wegen

$$\left(x^2, \mathfrak{F}_0(1,1;x)\right) = \int_0^1 x^2 \, dx = \tfrac{1}{3}$$

$$\left(\mathfrak{F}_0(1,1;x), \mathfrak{F}_0(1,1;x)\right) = 1$$

und $\mathfrak{F}_2(1,1;x) = x^2 - x + \frac{1}{6}$:

$$\frac{1}{6} = |p_0^{(2)}| \neq \frac{(x^2, \mathfrak{F}_0)}{(\mathfrak{F}_0, \mathfrak{F}_0)} = \frac{1}{3}.$$

Zusammenfassend können wir formulieren:

Satz II. *Unter den klassischen orthogonalen Polynomsystemen*

$$\{P_n(x)\}, \{\mathfrak{F}_n(\alpha, \gamma; x)\}, \{L_n^{(\alpha)}(x)\}, \{H_n\}, \{T_n\}, \{C_n^{(\nu)}\}$$

bilden das System der LAGUERRE*schen Polynome* $\{L_n^{(\alpha)}(x)\}$ *und das System der* HERMITE*schen Polynome* $\{H_n(x)\}$ *die einzigen involutorischen Polynomsysteme.*

§ 4. Das den Laguerreschen und Hermiteschen Polynomen übergeordnete Polynomsystem $\{P_{k,n}(x)\}$

Wie in der Einleitung erwähnt wurde, existiert ein von einem ganzzahligen Parameter $k \geqq 1$ abhängiges orthogonales Polynomsystem $\{P_{k,n}(x)\}$,

das für $k=1$ und $k=2$ das LAGUERREsche ($\alpha=0$) bzw. HERMITEsche System enthält:

$$\{P_{1,n}(x)\}=\{L_n(x)\},\qquad \{P_{2,n}(x)\}=\{H_n(x)\}.$$

Das System $\{P_{k,n}(x)\}$ ist mit der Belegungsfunktion $p(z)=e^{-z^k}$ orthogonal auf einem k-strahligen symmetrischen Integrationsstern der z-Ebene $\mathfrak{S}=\bigcup_{\lambda=0}^{k-1}\mathfrak{S}_\lambda$, wo $\mathfrak{S}_\lambda$ den Strahl $[z]=\left[e^{\frac{2\pi i}{k}\lambda}\cdot r\right]_{\leq r\leq\infty}$ bedeutet:

$$\left(P_{k,n}(z),P_{k,m}(z)\right)^{(k)}_{e^{-z^k}}=\sum_{\lambda=0}^{k-1}\int\limits_{\mathfrak{S}_\lambda}^{0\ \infty}P_{k,n}(z)\,\overline{P_{k,m}(z)}\,e^{-z^k}\,dr=0\qquad m\neq n.$$

Die Polynome $P_{k,n}(x)$ lauten, wenn wir $n=n_k^*+n_k k$ setzen $(0\leq n_k^*<k)$

$$P_{k,n}(x)=n_k!\cdot\sum_{\nu=0}^{n_k}\frac{(-)^{n_k-\nu}}{\nu!}\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k-\nu}x^{n_k^*+\nu k},\tag{6}$$

ihre Norm ist

$$(P_{k,n},P_{k,n})^{(k)}_{e^{-z^k}}=k\cdot(n_k!)^2\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k}\int_0^\infty r^{2n_k^*}e^{-r^k}\,dr.$$

Da die Polynomsysteme $\{P_{1,n}(x)\}$ und $\{P_{2,n}(x)\}$ involutorisch sind, liegt die Frage nahe, ob dies auch für alle k der Fall ist. Zur Anwendung des Kriteriums (5) berechnen wir das skalare Produkt:

$$\left(z^n,P_{k,\nu}(z)\right)=\sum_{\lambda=0}^{k-1}\int\limits_{\mathfrak{S}_\lambda}^{0\ \infty}z^n\,\overline{P_{k,\nu}(z)}\,e^{-r^k}\,dr$$

$$=\nu_k!\sum_{\lambda=0}^{k-1}\sum_{\varkappa=0}^{\nu_k}\frac{(-)^{\nu_k-\varkappa}}{\varkappa!}\binom{\nu_k+\frac{2\nu_k^*+1}{k}-1}{\nu_k-\varkappa}\int_0^\infty\left(re^{\frac{2\pi i}{k}\lambda}\right)^n\overline{\left(r\cdot e^{\frac{2\pi i}{k}\lambda}\right)^{\nu_k^*+\varkappa k}}\cdot e^{-r^k}\,dr$$

$$=\nu_k!\sum_{\varkappa=0}^{\nu_k}\frac{(-)^{\nu_k-\varkappa}}{\varkappa!}\binom{\nu_k+\frac{2\nu_k^*+1}{k}-1}{\nu_k-\varkappa}\cdot\int_0^\infty r^{n+\nu_k^*+\varkappa k}\left\{\sum_{\lambda=0}^{k-1}\left[e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)}\right]^\lambda\right\}e^{-r^k}\,dr.$$

Da

$$\sum_{\lambda=0}^{k-1}\left[e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)}\right]^\lambda=\begin{cases}\sum_{\lambda=0}^{k-1}1=k & \text{für } \nu\equiv n\,(k)\\ \dfrac{e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)\cdot k}-1}{e^{\frac{2\pi i}{k}(n-\nu_k^*-\varkappa k)}-1}=0 & \text{für } \nu\not\equiv n\,(k)\end{cases}\tag{7}$$

ist $(z^n,P_{k,\nu})^{(k)}_{e^{-z^k}}\neq 0$ nur für $\nu\equiv n\,(k)$. Für diesen Fall gilt also

$$(z^n,P_{k,\nu})^{(k)}_{e^{-z^k}}=k\cdot\nu_k!\sum_{\varkappa=0}^{\nu_k}\frac{(-)^{\nu_k-\varkappa}}{\varkappa!}\binom{\nu_k+\frac{2\nu_k^*+1}{k}-1}{\nu_k-\varkappa}\int_0^\infty r^{n+\nu_k^*+\varkappa k}e^{-r^k}\,dr.$$

Setzen wir $\Gamma_k(z) = \int_0^\infty r^{z-1} e^{-r^k}\, dr$, so erhalten wir durch Rückführung auf die Γ-Funktion $(k=1)$ die Funktionalgleichung:

$$\Gamma_k(z) = \frac{\overline{z-k}\cdot\overline{z-2k}\dots\overline{z-\lambda k}}{k^\lambda}\cdot\Gamma_k(z-\lambda k)$$

(für $k=1$ liegt die Funktionalgleichung der Γ-Funktion vor) und damit für

$$\int_0^\infty r^{2n_k^*+(n_k+\varkappa)k} e^{-r^k}\, dr = \frac{\overline{2n_k^*+1+\overline{n_k+\varkappa-1}\cdot k}\dots\overline{2n_k^*+1}}{k^{n_k+\varkappa}}\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr$$

$$= \binom{n_k+\varkappa+\frac{2n_k^*+1}{k}-1}{n_k+\varkappa}(n_k+\varkappa)!\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr.$$

Es wird also

$$\left(z^n, P_{k,\nu}\right)^{(k)}_{e^{-z^k}} = \nu_k!\cdot k\cdot\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr \times$$

$$\times\sum_{\varkappa=0}^{\nu_k}\frac{(-)^{\nu_k-\varkappa}}{\varkappa!}\binom{\nu_k+\frac{2n_k^*+1}{k}-1}{\nu_k-\varkappa}(n_k+\varkappa)!\binom{n_k+\varkappa+\frac{2n_k^*+1}{k}-1}{n_k+\varkappa}$$

$$= \nu_k!\cdot k\cdot\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr\cdot(-)^{\nu_k}\cdot n_k!\binom{\nu_k+\frac{2\nu_k^*+1}{k}-1}{\nu_k}\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k}\times$$

$$\times F\left(-\nu_k,\ n_k+\frac{2n_k^*+1}{k},\ \frac{2n_k^*+1}{k};\ 1\right)$$

$$= k\cdot\nu_k!\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr\binom{n_k}{\nu_k}\frac{\Gamma\left(n_k+\frac{2n_k^*+1}{k}\right)}{\Gamma\left(\frac{2n_k^*+1}{k}\right)}.$$

Nun ist nach (6) $p_\nu^{(n)}=0$ für $\nu\not\equiv n(k)$ und damit nach (7) die Beziehung (5) für solche ν immer erfüllt. Ist $\nu\equiv n(k)$, so lautet (5) für n und $\nu=n_k^*+\varkappa k$ $(n=0,1,2,\dots;\ \varkappa=0,1,\dots,n_k)$, da

$$\left(P_{k,n_k^*+\varkappa k}, P_{k,n_k^*+\varkappa k}\right)^{(k)}_{e^{-z^k}} = k(\varkappa!)^2\binom{\varkappa+\frac{2n_k^*+1}{k}-1}{\varkappa}\int_0^\infty r^{2n_k^*} e^{-r^k}\, dr$$

ist:

$$C_n\cdot C_{n_k^*+\varkappa k}\cdot n_k!\frac{(-)^{n_k-\varkappa}}{\varkappa!}\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k-\varkappa} = \frac{n_k!\binom{n_k+\frac{2n_k^*+1}{k}-1}{n_k}\binom{n_k}{\varkappa}}{\varkappa!\binom{\varkappa+\frac{2n_k^*+1}{k}-1}{\varkappa}}$$

oder:

(8) $$C_n\cdot C_{n_k^*+\varkappa k} = (-)^{n_k}\cdot(-)^\varkappa \qquad (n=0,1,\dots;\ \varkappa=0,1,\dots,n_k).$$

Diese Gleichung kann durch verschiedene Vorzeichensysteme $\{c_n\}$ gelöst werden. Setzen wir $\varkappa = 0$, so folgt $c_n = (-)^{n_k} v_{n_k^*}$. Wie wir auch bei k Vorzeichen $\{c_0, c_1, \ldots, c_{k-1}\}$" wählen, stets ist (8) durch $c_n = (-)^{n_k} v_{n_k^*}$ $(n = 0, 1, \ldots)$ gelöst, und alle Lösungen lassen sich auch so darstellen. Es gilt also: für alle k $(k = 1, 2, \ldots)$:

Das Polynomsystem $\{P_{k,n}(x)\}$ ist involutorisch. Es besitzt genau 2^k involutorische Formen.

Das einfachste System ergibt sich mit $c_0 = c_1 = \cdots = c_{k-1} = 1$.

$$P^*_{k,n}(x) = n_k! \sum_{\nu=0}^{n_k} \frac{(-)^\nu}{\nu!} \binom{n_k + \dfrac{2n_k^* + 1}{k} - 1}{n_k - \nu} x^{n_k^* + \nu k}.$$

Für $k = 1$ und $k = 2$ erhält man hieraus gerade die in § 1 bzw. § 3 angegebenen involutorischen Formen der LAGUERREschen bzw. HERMITEschen Polynome.

Gießen, Mathematisches Institut der Universität

(Eingegangen am 15. September 1955)

SCHOENEBERG, B.
Math. Zeitschr. Bd. 65, S. 16—24 (1956)

Über die Diskriminante der elliptischen Funktionen und ihre Quadratwurzel

Von

BRUNO SCHOENEBERG

Die Fourier-Koeffizienten von

$$\Delta(\tau) = e^{2\pi i\tau} \prod_{n=1}^{\infty} (1 - e^{2\pi i\tau n})^{24} = \sum_{n=1}^{\infty} \tau(n)\, e^{2\pi i\tau n}, \qquad \Im\mathfrak{m}\,\tau > 0$$

sind ihrer arithmetischen Natur nach noch nicht in wünschenswertem Umfange bekannt. Man weiß durch MORDELL[1]), daß zwischen ihnen folgende Beziehungen bestehen:

(1) $\tau(m\,n) = \tau(m)\,\tau(n)$ bei $(m, n) = 1$,

(2) $\tau(p^{\alpha}) = \tau(p)\,\tau(p^{\alpha-1}) - p^{11}\tau(p^{\alpha-2})$ bei primem p und ganzem $\alpha \geqq 2$.

Dieses Ergebnis hat HECKE[2]) erneut hergeleitet im Rahmen einer allgemeineren Theorie, der man unter anderem entnimmt, daß eine (1) und (2) entsprechende Beziehung auch für

$$\sqrt{\Delta(\tau)} = e^{\frac{2\pi i\tau}{2}} \prod_{n=1}^{\infty} (1 - e^{2\pi i\tau n})^{12} = \sum_{\substack{n=1 \\ n\equiv 1\,(2)}}^{\infty} \tau_2(n)\, e^{\frac{2\pi i\tau}{2}n}, \qquad \Im\mathfrak{m}\,\tau > 0$$

gilt. Es ist nämlich

(3) $\tau_2(m\,n) = \tau_2(m)\,\tau_2(n)$ bei $(m, n) = 1$,

(4) $\tau_2(p^{\alpha}) = \tau_2(p)\,\tau_2(p^{\alpha-1}) - p^5\,\tau_2(p^{\alpha-2})$ bei primem $p \neq 2$ und $\alpha \geqq 2$.

Durch (1) und (3) ist die Frage nach dem Verschwinden von $\tau(n)$ und $\tau_2(n)$ auf die Frage nach dem Verschwinden von $\tau(p^{\alpha})$ und $\tau_2(p^{\alpha})$ zurückgeführt. Nun ist nach MORDELL[1])

(5) $$\tau(p^{\alpha}) = \frac{p^{\frac{11}{2}\alpha} \sin(\alpha+1)\,\Theta_p}{\sin\Theta_p} \quad \text{mit} \quad 2\cos\Theta_p = \frac{\tau(p)}{p^{\frac{11}{2}}}, \quad (\alpha \geqq 0),$$

[1]) MORDELL, L. J.: On Mr. Ramanujan's empirical expansions of modular functions. Proc. Cambridge Philos. Soc. **19**, 117—124 (1917).

[2]) HECKE, E.: Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung. I, II. Math. Ann. **114**, 1—28, 316—351 (1937).

wie man sofort bestätigt, wenn man diesen Ausdruck für $\tau(p^\alpha)$ in (?) einsetzt. Entsprechend folgt aus (4)

$$(6) \qquad \tau_2(p^\alpha) = \frac{p^{\frac{5}{2}\alpha} \sin(\alpha+1)\Theta'_p}{\sin \Theta'_p} \qquad \text{mit} \qquad 2\cos\Theta'_p = \frac{\tau_2(p)}{p^{\frac{5}{2}}}.$$

Aus (5) folgt, wie LEHMER[3]) gezeigt hat, daß, wenn $\tau(n)$ überhaupt einmal verschwindet, das kleinste derartige n eine Primzahl ist. Bei verschwindendem $\tau(p^\alpha)$ ist nämlich Θ_p reell, also $\left|\frac{\tau(p)}{p^{\frac{11}{2}}}\right| \leq 2$. Andererseits ist bei verschwindendem $\tau(p^\alpha)$, wie sich aus (2) ergibt, $\frac{\tau(p)}{p^{\frac{11}{2}}}$ ganz-algebraisch. Also ist in $\left(\frac{\tau(p)}{p^{\frac{11}{2}}}\right)^2 - r = 0$ das rationale r eine ganze Zahl. Überdies ist $0 \leq r \leq 4$. Hier sind $r=1$ und 4 nicht möglich, weil $p^{\frac{11}{2}}$ nicht rational ist, und $r=2$ und 3 nicht, weil $\tau(2) \neq \pm 2^6$ und $\tau(3) \neq \pm 3^6$ ist. Also ist $\tau(p^\alpha)=0$ bei $\tau(p) \neq 0$ nicht möglich. Auf völlig entsprechende Weise ergibt sich: Das kleinste $n \equiv 1(2)$ mit $\tau_2(n)=0$ ist eine Primzahl. Ob es ein verschwindendes $\tau(n)$ oder ein verschwindendes $\tau_2(n)$ mit $n \equiv 1(2)$ gibt, weiß man nicht. Für $\tau(n)$ ist eine Reihe von Kongruenzeigenschaften bekannt, aus denen für das Verschwinden von $\tau(n)$ einschränkende Bedingungen folgen. In der vorliegenden Arbeit wird eine weitere Kongruenzeigenschaft hergeleitet. Da bei $\tau_2(n)$ ähnliche Probleme wie bei $\tau(n)$ vorliegen, soll hier auch die Funktion $\sqrt[]{\Delta(\tau)}$ nach derselben Methode untersucht werden.

Die Fourier-Koeffizienten von $\Delta(\tau)$ und $\sqrt[]{\Delta(\tau)}$ werden hier mit Hilfe gewisser positiv-definiter quadratischer Formen in 8 und 4 Variablen unter Heranziehung von Kugelfunktionen gewonnen. Dazu sei an folgenden Sachverhalt erinnert[4]):

Es sei $\mathfrak{A} = (a_{ik})$ eine ganzzahlige symmetrische Matrix mit $2r$ Zeilen und Spalten und $a_{ii} \equiv 0(2)$; die quadratische Form $\sum_{i,k=1}^{2r} a_{ik} x_i x_k$ sei positiv-definit; die Determinante von $\mathfrak{A}$ sei $|a_{ik}| = D$ und $(a_{ik})^{-1} = \frac{1}{D}(A_{ik})$. Der größte gemeinsame Teiler $\left(\frac{A_{11}}{2}, \ldots, \frac{A_{2r,2r}}{2}, \ldots, A_{ik} \ldots\right)$ sei K, und es sei $N = D/K$. Ferner sei $P_\nu(\mathfrak{x})$ eine Kugelfunktion in $\mathfrak{x} = (x_1, \ldots, x_{2r})$ in bezug auf $\sum_{i,k=1}^{2r} a_{ik} x_i x_k$ von der Dimension ν. Damit ist gemeint, daß $P_\nu(\mathfrak{x})$ durch eine Transformation, welche $\sum a_{ik} x_i x_k$ in eine Summe von Quadraten transformiert, zu einer gewöhnlichen Kugelfunktion in den neuen Variablen wird. Weiter sei $\mathfrak{h}$ ein ganz-

---

[3]) LEHMER, D. H.: The vanishing of Ramanujan's function $\tau(n)$. Duke Math. J. **14**, 429—433 (1947).

[4]) SCHOENEBERG, B.: Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen. Math. Ann. **116**, 511—523 (1939).

zahliger $2r$-dimensionaler Vektor mit $\mathfrak{A}\mathfrak{h} \equiv 0(N)$. Dann ist mit $(\mathfrak{n} = n_1, \ldots, n_{2r})$

$$(7)\qquad \begin{cases} \vartheta(\tau; \mathfrak{h}, \mathfrak{A}, P_\nu) = \sum\limits_{\mathfrak{n} \equiv \mathfrak{h}(N)} P_\nu(\mathfrak{n})\, e^{2\pi i \tau \frac{\frac{1}{2}\sum a_{ik} n_i n_k}{N^2}} = \sum\limits_{n=0}^{\infty} c_{P_\nu}(n)\, e^{\frac{2\pi i \tau}{N} n}, \\ c_{P_\nu}(n) = \sum\nolimits^{*} P_\nu(\mathfrak{n}), \end{cases}$$

wo für $c_{P_\nu}(n)$ über alle $\mathfrak{n} \equiv \mathfrak{h}(N)$ mit $\frac{1}{2N} \sum\limits_{i,k=1}^{2r} a_{ik} n_i n_k = n$ zu summieren ist, eine ganze Modulform der Dimension $-(r+\nu)$ zur Stufe N.

Daß für die Kugelfunktionen $(\sum a_{ik} l_i x_k)^\nu$ mit $\sum a_{ik} l_i l_k = 0$ auf diese Weise Modulformen entstehen, folgt aus dem Ansatz. Es führen aber alle Kugelfunktionen in bezug auf $\sum a_{ik} x_i x_k$ zu Modulformen, weil jede Kugelfunktion der Dimension ν linear homogen durch die $(\sum a_{ik} l_i x_k)^\nu$ mit der angegebenen Bedingung für die l_i ausdrückbar ist.

Für das Folgende brauchbare spezielle Kugelfunktionen in bezug auf $\sum a_{ik} x_i x_k = 2\boldsymbol{Q}(\mathfrak{x})$ gewinnt man durch den Ansatz

$$P_\nu(\mathfrak{x}) = \sum_{j=0}^{[\nu/2]} a_j x_1^{\nu-2j} \boldsymbol{Q}(\mathfrak{x})^j, \qquad \sum_{i=1}^{2r} \frac{\partial^2}{\partial y_i} P_\nu(\mathfrak{x}) = 0.$$

Dabei ist $x_i = \sum\limits_{k=1}^{2r} t_{ik} y_k$ eine Transformation, durch die $\sum\limits_{i,k=1}^{2r} a_{ik} x_i x_k = \sum\limits_{i=1}^{2r} y_i^2$ wird. Man erhält eine Rekursionsformel für die Koeffizienten a_j und damit

$$(8)\qquad P_\nu(\mathfrak{x}) = \sum_{j=0}^{[\nu/2]} \frac{(-1)^j}{j!} \left(\frac{A_{11}}{2D}\right)^j \frac{\nu(\nu-1)\ldots(\nu-2j+1)}{(r+\nu-2)\ldots(r+\nu-j-1)} \boldsymbol{Q}(\mathfrak{x})^j.$$

Um eine Entwicklung für $\Delta(\tau)$ zu erhalten, setzt man in (7) für $\mathfrak{A}$ die bekannte Matrix

$$\mathfrak{A}_8 = \begin{bmatrix} 2, & 1, & 0, & . & . & . & . & 0 \\ 1, & 4, & 1, & & & & & . \\ 0, & 1, & 12, & 3, & & & & . \\ 0, & 0, & 3, & 20, & 5, & & & . \\ 0, & & & 5, & 4, & 3, & & . \\ 0, & & & & 3, & 4, & 1, & . \\ 0, & & & & & 1, & 2, & 1 \\ 0, & . & . & . & . & . & 1, & 2 \end{bmatrix} \quad \text{mit} \quad D = K = N = 1$$

und für $P_\nu(\mathfrak{x})$ eine Kugelfunktion der Dimension 8 in bezug auf $\mathfrak{A}_8$. Dann ist die Funktion (7) eine ganze Modulform der Dimension -12 zur Stufe 1, die in der Spitze des Fundamentalbereichs verschwindet und daher, wenn sie nicht identisch verschwindet, bis auf einen konstanten Faktor gleich $\Delta(\tau)$ ist.

Die mit $\mathfrak{A}_8$ gebildeten Reihen (7) verschwinden für $\nu < 8$ identisch, und zwar für ungerades ν trivialerweise und für gerades ν als Spitzenformen einer Dimension > -12 zur Stufe 1. Es ist vorteilhaft, auch ihre Reihenentwicklungen heranzuziehen.

Die ersten vier Kugelfunktionen in bezug auf $\mathfrak{A}_8$ von gerader Dimension sind nach (8) mit $A_{11} = 2$

$$(9)\quad \begin{cases} P_2(\mathfrak{x}) = x_1^2 - \frac{1}{2}\,\boldsymbol{Q}_8(\mathfrak{x}) \\ P_4(\mathfrak{x}) = x_1^4 - 2\,x_1^2\,\boldsymbol{Q}_8(\mathfrak{x}) + \frac{2}{5}\,\boldsymbol{Q}_8(\mathfrak{x})^2 \\ P_6(\mathfrak{x}) = x_1^6 - \frac{15}{4}\,x_1^4\,\boldsymbol{Q}_8(\mathfrak{x}) + \frac{45}{14}\,x_1^2\,\boldsymbol{Q}_8(\mathfrak{x})^2 - \frac{5}{14}\,\boldsymbol{Q}_8(\mathfrak{x})^4 \\ P_8(\mathfrak{x}) = x_1^8 - \frac{28}{5}\,x_1^6\,\boldsymbol{Q}_8(\mathfrak{x}) + \frac{28}{3}\,x_1^4\,\boldsymbol{Q}_8(\mathfrak{x})^2 - \frac{14}{3}\,x_1^2\,\boldsymbol{Q}_8(\mathfrak{x})^3 + \frac{1}{3}\,\boldsymbol{Q}_8(\mathfrak{x})^4. \end{cases}$$

Die Bedingung $\mathfrak{A}\mathfrak{h} = 0\,(N)$ entfällt hier. Die mit $\nu = 0$ gebildete Reihe ist

$$\sum_{\mathfrak{n}} e^{2\pi i \tau \boldsymbol{Q}_8(\mathfrak{n})} = \sum_{n=0}^{\infty} z_8(n)\, e^{2\pi i \tau n},$$

wo $z_8(n)$ gleich der Anzahl der ganzzahligen Lösungen $\mathfrak{n}$ von $\boldsymbol{Q}_8(\mathfrak{n}) = n$ ist. Diese Reihe ist bis auf einen konstanten Faktor gleich der Eisensteinschen Reihe der Dimension -4. Das ergibt wegen $z_8(1) = 240$

$$(10)\qquad z_8(n) = 240\,\sigma_3(n),$$

wo, wie üblich, $\sigma_k(n) = \sum_{\substack{d>0 \\ d\mid n}} d^k$ ist. Benutzt man diesen Wert für $z_8(n)$, so folgen aus dem identischen Verschwinden der mit P_2, P_4, P_6 gebildeten Reihen nacheinander folgende Relationen:

$$(11)\quad \begin{cases} \sum\limits_{\boldsymbol{Q}_8(\mathfrak{n})=n} n_1^2 = 120\,n\,\sigma_3(n), \\ \sum\limits_{\boldsymbol{Q}_8(\mathfrak{n})=n} n_1^4 = 144\,n^2\,\sigma_3(n), \\ \sum\limits_{\boldsymbol{Q}_8(\mathfrak{n})=n} n_1^6 = 240\,n^3\,\sigma_3(n). \end{cases}$$

Zur Berechnung jeder dieser Relationen werden die vorangehenden benutzt. Aus ihnen folgt mit P_8 aus (9)

$$\sum_{\mathfrak{n}} P_8(\mathfrak{n})\, e^{2\pi i \tau \boldsymbol{Q}_8(\mathfrak{n})} = \sum_{n=1}^{\infty} c_n\, e^{2\pi i \tau n}, \qquad c_n = \sum_{\boldsymbol{Q}_8(\mathfrak{n})=n} n_1^8 - 480\,n^4\,\sigma_3(n).$$

Hier ist $c_1 = 144$. Denn aus $\sum\limits_{\boldsymbol{Q}_8=1} n_1^2 = 120$ und $\sum\limits_{\boldsymbol{Q}_8=1} n_1^4 = 144$ folgt, daß es 112 Lösungen von $\boldsymbol{Q}_1^8(\mathfrak{n}) = 1$ mit $n_1 = 1$ und 2 Lösungen mit $n_2 = 2$ gibt. Also ist $\sum\limits_{\boldsymbol{Q}_8=1} n^2 = 624$. Damit ist[5])

$$(12)\qquad \tau(n) = \frac{1}{144}\left\{ \sum_{\boldsymbol{Q}_8(\mathfrak{n})=n} n_1^8 - 480\,n^4\,\sigma_3(n) \right\}.$$

[5]) Vgl. hierzu Hecke, E.: Analytische Theorie der positiven quadratischen Formen. Kgl. Danske Vidensk. Selsk. Math.-phys. Medd. **17**, 12 (1940), bes. S. 86—89.

Eine weitere Darstellung von $\Delta(\tau)$ gewinnt man mit Hilfe der quadratischen Form in 16 Variablen

$$Q_{16}(\mathfrak{x}) = Q_8(\mathfrak{x}_1) + Q_8(\mathfrak{x}_2)$$

mit dem schon eingeführten Q_8 und $\mathfrak{x}_1 = (x_1, \ldots, x_8)$, $\mathfrak{x}_2 = (x_9, \ldots, x_{16})$, $\mathfrak{x} = (x_1, \ldots, x_{16})$. Für diese Form ist

$$\mathfrak{A}_{16} = \begin{pmatrix} \mathfrak{A}_8 & 0 \\ 0 & \mathfrak{A}_8 \end{pmatrix}, \qquad D = K = N = 1.$$

Die ersten beiden Kugelfunktionen gerader Dimension sind

$$\begin{cases} P_2'(\mathfrak{x}) = x_1^2 - \frac{1}{4} Q_{16}(\mathfrak{x}), \\ P_4'(\mathfrak{x}) = x_1^4 - \frac{6}{5} x_1^2 Q_{16}(\mathfrak{x}) + \frac{2}{15} Q_{16}(\mathfrak{x})^2. \end{cases} \tag{13}$$

Die mit $\nu = 0$ gebildete Reihe (7) ist bis auf einen konstanten Faktor gleich der Eisensteinschen Reihe der Dimension -8. Das ergibt für die Anzahl $z_{16}(n)$ der Lösungen von $Q_{16}(\mathfrak{n}) = n$

$$z_{16}(n) = 480\,\sigma_7(n). \tag{14}$$

Die mit $P_2'(\mathfrak{x})$ gebildete Reihe verschwindet als Spitzenform der Dimension -10 identisch. Also ist

$$\sum_{Q_{16}(\mathfrak{n})=n} n_1^2 = 120\,n\,\sigma_7(n). \tag{15}$$

Damit folgt für die Koeffizienten c_n' der mit $P_4'(\mathfrak{x})$ gebildeten Reihe

$$\sum_{\mathfrak{n}} P_4'(\mathfrak{n})\, e^{2\pi i \tau Q_{16}(\mathfrak{n})} = \sum_{n=1}^{\infty} c_n' e^{2\pi i \tau n}, \qquad c_n' = \sum_{Q_{16}(\mathfrak{n})=n} n_1^4 - 80\,n^2\,\sigma_7(n).$$

Hier ist $c_1' = 64$, also ist die Reihe eine nicht identisch verschwindende Spitzenform der Dimension -12 und damit

$$\tau(n) = \frac{1}{64}\left\{ \sum_{Q_{16}(\mathfrak{n})=n} n_1^4 - 80\,n^2\,\sigma_7(n) \right\}. \tag{16}$$

Zur weiteren Untersuchung von $\tau(n)$ werde $\sum_{Q_{16}(\mathfrak{n})=n} n_1^4$ umgeformt. Es ist

$$\sum_{Q_{16}(\mathfrak{n})=n} n_1^4 = \sum_{Q_8(\mathfrak{n}_1)=n} n_1^4 + \sum_{Q_8(\mathfrak{n}_1)=n-1} n_1^4 \cdot z_8(1) + \sum_{Q_8(\mathfrak{n}_1)=n-2} n_1^4 \cdot z_8(2) + \cdots$$

$$= \sum_{Q_8(\mathfrak{n}_1)=n} n_1^4 + \sum_{i=1}^{n-1} \sum_{Q_8(\mathfrak{n}_1)=n-i} n_1^4\, z_8(i).$$

Damit ist nach (11) und (10)

$$\sum_{Q_{16}(\mathfrak{n})=n} n_1^4 = 144\,n^2\,\sigma_3(n) + 144 \cdot 240 \sum_{i=1}^{n-1} (n-i)^2\,\sigma_3(n-i)\,\sigma_3(i)$$

und nach (16)

$$\tau(n) = \tfrac{n^2}{4}\{9\sigma_3(n) - 5\sigma_7(n)\} + 9\cdot 240 \sum_{i=1}^{n-1} (n-i)^2\,\sigma_3(n-i)\,\sigma_3(i). \tag{17}$$

Das ergibt für $\tau(n)$ die *Kongruenzeigenschaft*

$$\tau(n) \equiv \tfrac{n^2}{4}\{9\sigma_3(n) - 5\sigma_7(n)\} \bmod 9\cdot 240. \tag{18}$$

Für eine Primzahl $p \neq 2, 3, 5$ ist also $\tau(p)$ höchstens dann gleich Null, wenn die Kongruenz

$$5p^7 - 9p^3 - 4 \equiv 0 \bmod 2^6\cdot 3^3\cdot 5$$

erfüllt ist, d.h. höchstens für

$$p \equiv -1 \bmod 2^2\cdot 3^3\cdot 5. \tag{19}$$

Das ist eine Kongruenzeigenschaft von bekanntem Typus. Die Methode ihrer Herleitung ist auch auf die Funktion $\sqrt{\Delta(\tau)}$ anwendbar.

$\sqrt{\Delta(\tau)}$ ist eine ganze Modulform der Dimension -6 zur Stufe 2, die in allen Spitzen des Fundamentalbereiches verschwindet, und dadurch bis auf einen konstanten Faktor bestimmt. Zu ihrer Darstellung wird die quadratische Form $\boldsymbol{Q}_4(\mathfrak{x})$ mit

$$\mathfrak{A}_4 = \begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix}, \quad D = 4,\ K = N = 2$$

herangezogen. Die Kugelfunktionen bezüglich dieser Form von der zweiten und vierten Dimension sind

$$\begin{cases} R_2(\mathfrak{x}) = x_1^2 - \tfrac{1}{2}\boldsymbol{Q}_4(\mathfrak{x}), \\ R_4(\mathfrak{x}) = x_1^4 - \tfrac{3}{2}x_1^2\boldsymbol{Q}_4(\mathfrak{x}) + \tfrac{1}{4}\boldsymbol{Q}_4(\mathfrak{x})^2. \end{cases} \tag{20}$$

Eine brauchbare Lösung von $\mathfrak{A}_4\mathfrak{h} \equiv 0\,(2)$ ist $\mathfrak{h} \equiv (1, 1, 0, 0) \bmod 2$. Die mit $\nu = 0$ gebildete Reihe ist

$$\sum_{\mathfrak{n} \equiv \mathfrak{h} \bmod 2} e^{\frac{2\pi i\tau}{2}\frac{\boldsymbol{Q}_4(\mathfrak{n})}{2}} = \sum_{n=0}^{\infty} z_4(n)\, e^{\frac{2\pi i\tau}{2}n},$$

in der nur Exponenten $n \equiv 1 \bmod 2$ auftreten. Die Anzahl $z_4(n)$ der Lösungen von $\frac{1}{2}\boldsymbol{Q}_4(\mathfrak{n}) = n$ mit $\mathfrak{n} \equiv \mathfrak{h} \bmod 2$ bestimmt man mit Hilfe der p-Teilwerte zur Stufe 2 zu

$$z_4(n) = 8\sigma_1(n), \quad n \equiv 1 \bmod 2. \tag{21}$$

Die Reihe mit $R_2(\mathfrak{x})$ ist als Spitzenform der Dimension -4 zur Stufe 2 identisch Null. Damit ist bei im folgenden immer als ungerade vorausgesetztem n

$$\sum_{\substack{\frac{1}{2}Q_4(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^2 = 8n\sigma_1(n). \tag{22}$$

Für die Koeffizienten d_n der mit $R_4(\mathfrak{x})$ gebildeten Reihe folgt bei Benutzung von (21) und (22)

$$\sum_{\mathfrak{n}\equiv\mathfrak{h} \bmod 2} R_4(\mathfrak{n})\, e^{\frac{2\pi i\tau}{2}\frac{Q_4(\mathfrak{n})}{2}} = \sum_{n=1}^{\infty} d_n e^{\frac{2\pi i\tau}{2}n}, \qquad d_n = \sum_{\substack{\frac{1}{2}Q_4(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^4 - 16n^2\sigma_1(n).$$

Hier ist $d_1 = -8$, wie aus (22) folgt, wenn man dort $n=1$ setzt. Damit ist

$$\tau_2(n) = -\frac{1}{8}\left\{\sum_{\substack{\frac{1}{2}Q_4(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^4 - 16n^2\sigma_1(n)\right\}. \tag{23}$$

Die Summe besteht aus $8\sigma_1(n)$ Summanden, die alle kongruent 1 mod 16 sind. Für den Fall, daß $\tau_2(n)=0$ ist, muß also $8\sigma_1(n)=0 \bmod 16$ sein. Daraus folgt: $\tau_2(n)$ *ist sicher dann von Null verschieden, wenn n eine ungerade Anzahl von Teilern hat, wenn also n ein Quadrat ist.*

Eine weitere Darstellung für $\sqrt[4]{\Delta(\tau)}$ gewinnt man durch die quadratische Form in 8 Variablen $Q_8'(\mathfrak{x}) = Q_4(\mathfrak{x}_1) + Q_4(\mathfrak{x}_2)$ mit

$$\mathfrak{A}_8' = \begin{bmatrix} \mathfrak{A}_4 & 0 \\ 0 & \mathfrak{A}_4 \end{bmatrix}, \qquad D=16,\ K=8,\ N=2.$$

Es werde $\mathfrak{h} \equiv (1, 1, 0, 0, \ldots, 0) \bmod 2$ gesetzt. Die Kugelfunktion der Dimension 2 ist jetzt

$$R_2'(\mathfrak{x}) = x_1^2 - \tfrac{1}{4} Q_8'(\mathfrak{x}). \tag{24}$$

Die Anzahl $z_8'(n)$ der Lösungen von $\frac{1}{2}Q_8'(\mathfrak{n}) = n$ mit $\mathfrak{n}\equiv\mathfrak{h} \bmod 2$ ist gleich

$$z_8'(n) = 8\sigma_3(n), \tag{25}$$

wie man sieht, wenn man die Eisensteinschen Reihen der Dimension -4 zur Stufe 2 heranzieht. Mit (24) und (25) ist

$$\sum_{\mathfrak{n}\equiv\mathfrak{h} \bmod 2} R_2'(\mathfrak{n})\, e^{\frac{2\pi i\tau}{2}\frac{Q_8'(\mathfrak{n})}{2}} = \sum_{n=1}^{\infty} d_n' e^{\frac{2\pi i\tau}{2}n}, \qquad d_n' = \sum_{\substack{\frac{1}{2}Q_8'(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^2 - 4n\sigma_3(n).$$

Wegen $d_1' = 4$ ist also

$$\tau_2(n) = \frac{1}{4}\left\{\sum_{\substack{\frac{1}{2}Q_8(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^2 - 4n\sigma_3(n)\right\}. \tag{26}$$

Die hier auftretende Summe läßt sich umformen zu

$$\sum_{\substack{\mathfrak{n} \\ \frac{1}{2}Q_8(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^2 = \sum_{\substack{n_1 \\ \frac{1}{2}Q_3(n_1)=n \\ n_1\equiv(1\,1\,0\,0) \bmod 2}} n_1^2 + \sum_{\substack{n_1 \\ \frac{1}{2}Q_4(n_1)=n-2 \\ n_1\equiv(1\,1\,0\,0) \bmod 2}} n_1^2 \cdot z_4'(2) + \sum_{\substack{n_1 \\ \frac{1}{2}Q_4(n_1)=n-4 \\ n_1\equiv(1\,1\,0\,0) \bmod 2}} n_1^2 \cdot z_4'(4) + \cdots.$$

Dabei ist $z_4'(2i)$ die Anzahl der Lösungen von $\frac{1}{2}Q_4(\mathfrak{n}_2) = 2i$ mit $\mathfrak{n}_2 \equiv (0\,0\,0\,0) \bmod 2$, also gleich $24\sigma_1'(i)$ mit $\sigma_1'(i) = \sum_{\substack{d|i,\ d>0 \\ d\equiv 1 \bmod 2}} d$. Hieraus und aus (22) folgt

$$\sum_{\substack{\mathfrak{n} \\ \frac{1}{2}Q_8(\mathfrak{n})=n \\ \mathfrak{n}\equiv\mathfrak{h} \bmod 2}} n_1^2 = 8n\,\sigma_1(n) + \sum_{i=1}^{\frac{n-1}{2}} 8(n-2i)\,\sigma_1(n-2i)\cdot 24\,\sigma_1'(i)$$

und schließlich

$$\tau_2(n) = n\left(2\sigma_1(n) - \sigma_3(n)\right) + 48\sum_{i=1}^{\frac{n-1}{2}} (n-2i)\,\sigma_1(n-2i)\,\sigma_1'(i). \tag{27}$$

Die Koeffizienten $\tau_2(n)$ besitzen demnach die *Kongruenzeigenschaft*

$$\tau_2(n) \equiv n\left(2\sigma_1(n) - \sigma_3(n)\right) \bmod 48. \tag{28}$$

Wenn für primzahliges $p \neq 2, 3$ der Koeffizient $\tau_2(p) = 0$ ist, besteht die Kongruenz

$$p^3 - 2p^2 - 1 \equiv 0 \bmod 48,$$

die nur für $p \equiv -1 \bmod 48$ erfüllt ist.

Eine weitere Darstellung von $\sqrt{\Delta(\tau)}$ gewinnt man durch die quadratische Form in 12 Variablen $Q_{12}(\mathfrak{x}) = Q_4(\mathfrak{x}_1) + Q_4(\mathfrak{x}_2) + Q_4(\mathfrak{x}_3)$, wenn man die Eisensteinsche Reihe $G_6(\tau) = \sum_{\substack{n=1 \\ n\equiv 1 \bmod 2}}^{\infty} \sigma_5(n)\, e^{\frac{2\pi i\tau}{2}n}$ der Dimension -6 zur Stufe 2 heranzieht. Durch Berechnung der ersten Koeffizienten erhält man

$$\sqrt{\Delta(\tau)} = G_6(\tau) - \frac{1}{2}\sum_{\substack{\mathfrak{n} \\ \mathfrak{n}_i\equiv(1\,1\,0\,0) \bmod 2}} e^{\frac{2\pi i\tau}{2}\cdot\frac{1}{2}Q_{12}(\mathfrak{n})}.$$

Diese Darstellung führt zu

$$\tau_2(n) = \sigma_5(n) - \tfrac{1}{2}z_{12}(n), \tag{29}$$

wo $z_{12}(n)$ die Anzahl der Lösungen von $\frac{1}{2}Q_{12}(\mathfrak{n}) = n$ mit $\mathfrak{n}_i \equiv (1\,1\,0\,0) \bmod 2$ ist. Wegen $z_{12}(n) \equiv 0 \bmod 8^3$, wie aus (21) folgt, ist

$$\tau_2(n) \equiv \sigma_5(n) \bmod 2^8. \tag{30}$$

Es kann danach $\tau_2(p)$ höchstens dann verschwinden, wenn $p \equiv -1 \bmod 2^8$ ist.

Schließlich ist noch eine Darstellung von $\sqrt{\Delta(\tau)}$ gegeben durch

$$\sqrt{\Delta(\tau)} = \frac{1}{8}\left\{ \sum_{\substack{\mathfrak{n} \\ \mathfrak{n}_1 \equiv (1100) \\ \mathfrak{n}_2 \equiv \mathfrak{n}_3 \equiv (0000) \bmod 2}} e^{\frac{2\pi i\tau}{2} \cdot \frac{1}{2} Q_{12}(\mathfrak{n})} - \sum_{\substack{\mathfrak{n} \\ \mathfrak{n}_4 \equiv (1100) \bmod 2}} e^{\frac{2\pi i\tau}{2} \cdot \frac{1}{2} Q_{12}(\mathfrak{n})} \right\}.$$

Daraus folgt

$$\tau_2(n) = \tfrac{1}{8}\left(z'_{12}(n) - z_{12}(n)\right), \tag{31}$$

wo $z'_{12}(n)$ die Anzahl der Lösungen von $\frac{1}{2}Q_{12}(\mathfrak{n}) = n$ mit $\mathfrak{n}_1 \equiv (1\,1\,0\,0)$, $\mathfrak{n}_2 \equiv \mathfrak{n}_3 \equiv (0\,0\,0\,0) \bmod 2$ ist.

Die benutzten Reihen $\vartheta(\tau; \mathfrak{h}, \mathfrak{A}, P_\nu)$ führten, soweit sie identisch verschwinden, zu Relationen zwischen Darstellungsanzahlen und Darstellungskomponenten. Diese gestatteten es dann, die Koeffizienten $\tau(n)$ und $\tau_2(n)$ durch Anzahlen und Komponenten auszudrücken. Die Komponenten traten in einer speziellen Form auf, die durch die gewählte Kugelfunktion bedingt war. Verallgemeinert man HECKEs Ansatz zur Konstruktion einer Basis von Kugelfunktionen für die Dimension 2 auf die Dimension ν, so erhält man Relationen, die sich von den hier auftretenden bis auf von n unabhängige Faktoren dadurch unterscheiden, daß x_1^ν durch ein Monom in $x_1, \ldots, x_{2\nu}$ des Grades ν ersetzt wird.

Hamburg, Mathematisches Seminar der Universität

(Eingegangen am 26. Oktober 1955)

Dold, A.
Math. Zeitschr. Bd. 65, S. 25—35 (1956)

Erzeugende der Thomschen Algebra $\mathfrak{N}$

Von
Albrecht Dold

Einleitung. In [8] hat R. Thom eine Äquivalenzrelation zwischen kompakten (nicht notwendig zusammenhängenden) differenzierbaren Mannigfaltigkeiten eingeführt, die sich, grob gesprochen, folgendermaßen beschreiben läßt: Zwei differenzierbare Mannigfaltigkeiten sind genau dann äquivalent („cobordantes"), wenn sie zusammen den Rand einer berandeten differenzierbaren Mannigfaltigkeit bilden. (Für eine präzise Definition und für das Folgende vgl. [8], Chap. IV.)

Die Äquivalenzklassen können in natürlicher Weise addiert und multipliziert werden und bilden einen Ring bezüglich dieser Verknüpfungen. Man erhält verschiedene Äquivalenzklassenmengen und verschiedene Ringe Ω oder $\mathfrak{N}$, je nachdem ob man orientierte oder nicht-orientierte Mannigfaltigkeiten betrachtet. Die topologische Dimension der Mannigfaltigkeiten definiert eine Graduierung der Ringe Ω und $\mathfrak{N}$: $\Omega = \sum_{k=0}^{\infty} \Omega^k$, $\mathfrak{N} = \sum_{k=0}^{\infty} \mathfrak{N}^k$.

Die Struktur von $\mathfrak{N}$ ist verhältnismäßig einfach: $\mathfrak{N}$ ist ein Polynomring in abzählbar vielen Variablen x_i über dem Primkörper der Charakteristik 2; x_i wird repräsentiert durch eine geeignet gewählte i-dimensionale Mannigfaltigkeit $P(i)$; i durchläuft alle natürlichen Zahlen, die nicht von der Form $2^l - 1$ sind.

In [8] hat Thom für alle geraden i und für $i = 5$ Mannigfaltigkeiten $P(i)$ angegeben, die die (nicht eindeutig festgelegten) Variablen x_i repräsentieren. In der vorliegenden Arbeit geschieht dies für die verbleibenden Fälle, d.h. für alle ungeraden $i \neq 2^l - 1$, $i > 5$ (s. Satz 3).

Die angegebenen Mannigfaltigkeiten $P(i)$, i ungerade $\neq 2^l - 1$, sind orientierbar. Sie definieren daher Elemente von Ω (und zwar von der Ordnung 2; s. H), die bei der natürlichen Abbildung $\Omega \to \mathfrak{N}$ in x_i übergehen. Dies liefert Aussagen über die nur teilweise bekannte Struktur (s. [8], S. 81) von Ω; z.B. ergibt sich: Ω^k ist nicht trivial für $k \geqq 8$, d.h. in jeder Dimension $k \geqq 8$ gibt es nicht-berandende orientierbare kompakte differenzierbare Mannigfaltigkeiten (s. H). —

Wir definieren und untersuchen nun zunächst eine Klasse von Mannigfaltigkeiten $\{P(m, n)\}$, unter denen die in der vorstehenden Einleitung genannten Mannigfaltigkeiten $P(i)$ vorkommen.

A. Definition und erste Eigenschaften von $P(m, n)$. S^m, $m \geqq 0$, sei die Einheitssphäre des $(m+1)$-dimensionalen euklidischen Raumes mit den Koordinaten $x_0, x_1, \ldots, x_m$. $PC(n)$, $n \geqq 0$, sei der komplexe projektive Raum

von n komplexen Dimensionen; wir beschreiben ihn durch homogene Koordinaten $z_0, z_1, \ldots, z_n$.

Der topologische Raum $P(m, n)$ [1]) entsteht aus dem topologischen Produkt $S^m \times PC(n)$ durch die Identifikation $(x, z) = (-x, \bar{z})$. Dabei bezeichnet $-x$ den Diametralpunkt von $x \in S^m$ und $\bar{z}$ ist derjenige Punkt aus $PC(n)$, dessen Koordinaten konjugiert komplex zu denen von $z \in PC(n)$ sind.

Bezüglich der Identifikationsabbildung $\Phi: S^m \times PC(n) \to P(m, n)$ ist $S^m \times PC(n)$ zweiblättrige Überlagerung von $P(m, n)$; die nicht-triviale Deckbewegung φ ist durch

$$\varphi(x, z) = (-x, \bar{z}), \qquad x \in S^m,\ z \in PC(n) \tag{1}$$

gegeben.

$S^m \times PC(n)$ kann — in der üblichen Weise — als (reell) analytische Mannigfaltigkeit aufgefaßt werden; φ ist dann eine analytische Abbildung. Vermöge der Abbildung Φ wird daher auch $P(m, n)$ zur (reell) analytischen Mannigfaltigkeit, und Φ selbst ist analytisch.

Die Abbildung $(x, z) \to x$ von $S^m \times PC(n)$ auf S^m geht bei der Identifikation Φ in eine Abbildung $p: P(m, n) \to PR(m)$ ($= m$-dimensionaler reeller projektiver Raum) über. p ist Projektion eines (analytischen) Faserraumes $\{P(m, n), p, PR(m), PC(n), Z_2\}$ [2]) (s. [3], § 2); das nicht-triviale Element der Strukturgruppe Z_2 ist die Selbstabbildung $z \to \bar{z}$ von $PC(n)$.

B. Zellenzerlegung und Homologie mod 2 von $P(m, n)$. Wir geben bekannte Zellenzerlegungen von S^m und $PC(n)$ an und gewinnen mit ihrer Hilfe eine Zellenzerlegung von $P(m, n)$.

S^m: Die durch $x_{i+1} = x_{i+2} = \cdots = x_m = 0$, $x_i > 0$ ($x_i < 0$) definierte Punktmenge von S^m ist eine offene i-Zelle C_i^+ (C_i^-). Die Zellen $C_i^\pm$, $i = 0, 1, \ldots, m$, bilden eine Zellenzerlegung von S^m (CW-Komplex im Sinne von J. H. C. WHITEHEAD [10]) und genügen bei geeigneter Orientierung den Berandungsrelationen $\partial C_i^+ = C_{i-1}^+ + C_{i-1}^-$, $\partial C_i^- = -(C_{i-1}^+ + C_{i-1}^-)$, $i = 1, 2, \ldots, m$. Im folgenden seien die Zellen $C_i^\pm$ ein für alle Male mit einer festen Orientierung dieser Art ausgestattet.

Die Diametralpunktvertauschung $x \to -x$, $x \in S^m$, ist eine Selbstabbildung der m-Sphäre, die die Orientierung erhält oder umkehrt, je nachdem ob m ungerade oder gerade ist. Bezüglich der Zellenzerlegung $\{C_i^\pm\}$ ist sie eine Zellenabbildung und führt $C_i^\pm$ in $(-1)^{i+1} C_i^\mp$ über.

$PC(n)$: Die durch $z_j = 1$, $z_{j+1} = z_{j+2} = \cdots = z_n = 0$ definierte Punktmenge von $PC(n)$ ist eine offene $2j$-Zelle D_j. Die Zellen D_j, $j = 0, 1, \ldots, n$, die wir uns mit einer festen Orientierung versehen denken, bilden eine Zellenzerlegung (CW-Komplex) von $PC(n)$ und genügen den Berandungsrelationen $\partial D_j = 0$.

---

[1]) $P(1, 2)$ ist die von WU in [12], Nr. 3c betrachtete Mannigfaltigkeit.

[2]) Dies sieht man leicht ein — wir werden es im folgenden nicht benutzen — wenn man beachtet, daß Φ jede offene Menge von der Form $U \times PC(n)$ topologisch abbildet, wo U eine offene Menge aus S^m ist, die keine Diametralpunkte enthält.

Die Selbstabbildungen $z \to \bar{z}$ von $PC(n)$ erhält die Orientierung oder kehrt sie um, je nachdem ob n gerade oder ungerade ist. [Dies erkennt man leicht, wenn man inhomogene Koordinaten $z_1 z_0^{-1}, z_2 z_0^{-1}, \ldots, z_n z_0^{-1}$ benutzt; die Funktionaldeterminante in einem „eigentlichen" Punkt $z_0 \neq 0$ ist $(-1)^n$.] Bezüglich der Zellenzerlegung $\{D_j\}$ ist sie eine Zellenabbildung und führt D_j in $(-1)^j D_j$ über.

$S^m \times PC(n)$: Die Produktzellen $C_i^{\pm} \times D_j$ bilden eine Zellenzerlegung von $S^m \times PC(n)$ und genügen den Berandungsrelationen

$$(2) \qquad \begin{cases} \partial(C_i^{\pm} \times D_j) = \pm\,(C_{i-1}^{+} \times D_j + C_{i-1}^{-} \times D_j) \\ \partial(C_0 \times D_j) = 0, \quad i = 1, 2, \ldots, m, \quad j = 0, 1, \ldots, n. \end{cases}$$

Die Selbstabbildung φ [s. (1)] von $S^m \times PC(n)$ ist eine Zellenabbildung und es gilt

$$(3) \qquad \varphi(C_i^{\pm} \times D_j) = (-1)^{i+j+1}\,(C_i^{\mp} \times D_j).$$

$P(m, n)$: Die Abbildung Φ: $S^m \times PC(n) \to P(m, n)$ bildet die Zellen $C_i^{\pm} \times D_j$ topologisch ab (vgl. Fußnote 2). Die Zellen $\Phi(C_i^{+} \times D_j)$ — wir bezeichnen sie mit (C_i, D_j) — bilden daher und wegen (3) eine Zellenzerlegung von $P(m, n)$, und Φ ist eine Zellenabbildung. Aus (2) erhält man durch Anwenden von Φ wegen (3) die Berandungsrelationen

$$(4) \qquad \begin{cases} \partial(C_i, D_j) = \left(1 + (-1)^{i+j}\right)(C_{i-1}, D_j) \\ \partial(C_0, D_j) = 0, \quad i = 1, 2, \ldots, m, \quad j = 0, 1, \ldots, n. \end{cases}$$

Es bezeichne $H(m, n) = \sum_{\nu} H_\nu(m, n)$ die direkte Summe der Homologiegruppen mod 2, $H^*(m, n) = \sum_{\nu} H^\nu(m, n)$ den Kohomologiering mod 2 von $P(m, n)$. Nach (4) sind alle Zellen (C_i, D_j) Zyklen mod 2. Ihre Homologieklassen $[C_i, D_j]$ bilden daher eine Basis von $H(m, n)$.

$H^*(m, n)$ ist seiner additiven Struktur nach nichts anderes als der Modul der Homomorphismen von $H(m, n)$ in den Primkörper K der Charakteristik 2; $\langle k, h \rangle$ bezeichne den Wert der Kohomologieklasse k auf der Homologieklasse h. Die durch

$$(5) \qquad \langle (c^i, d^j), [C_\mu, D_\nu] \rangle = \delta_\mu^i \cdot \delta_\nu^j, \quad i, \mu = 0, 1, \ldots, m, \quad j, \nu = 0, 1, \ldots, n,$$

definierten Kohomologieklassen (c^j, d^j) bilden eine Basis der additiven Struktur von $H^*(m, n)$.

$P(m, n)$ hat also mod 2 dieselben Homologiegruppen wie $PR(m) \times PC(n)$. In D werden wir sehen, daß auch die Kohomologieringe mod 2 dieser beiden Räume übereinstimmen.

C. *$P(m, n)$ ist genau dann orientierbar, wenn $m \neq n\,(2)$ oder $m = 0$ ist.* Denn genau dann ist nach (4) die einzige höchstdimensionale Zelle (C_m, D_n) ein Zykel.

D. Der Kohomologiering mod 2 von $P(m, n)$. Für $m' \leq m$ und $n' \leq n$ identifizieren wir $S^{m'} \times PC(n')$ mit der analytischen Untermannigfaltigkeit

$x_{m'+1} = x_{m'+2} = \cdots = x_m = 0$, $z_{n'+1} = z_{n'+2} = \cdots = z_n = 0$ von $S^m \times PC(n)$ und $P(m', n')$ mit der analytischen Untermannigfaltigkeit $\Phi(S^{m'} \times PC(n'))$ von $P(m, n)$ (s. A). $P(m', n')$ repräsentiert die Homologieklasse $[C_{m'}, D_{n'}] \in H(m, n)$ (s. B). Wir werden, um den Schnitt der Homologieklassen $[C_i, D_j]$ und $[C_{i'}, D_{j'}]$, $i, i' \leqq m$, $j, j' \leqq n$, zu bestimmen, die Mannigfaltigkeit $P(i', j')$ in eine andere analytische Untermannigfaltigkeit von $P(m, n)$ deformieren, die sich in allgemeiner Lage relativ zu $P(i, j)$ befindet.

Es seien σ bzw. τ Permutationen der Zahlen 0, 1, 2, ..., m, bzw. 0, 1, 2, ..., n. Durch

$$x_0 \to \operatorname{sign}(\sigma)\, x_{\sigma(0)}, \quad x_\mu \to x_{\sigma(\mu)}, \quad \mu > 0, \tag{6}$$

$$z_0 \to \operatorname{sign}(\tau)\, z_{\tau(0)}, \quad z_\nu \to z_{\tau(\nu)}, \quad \nu > 0, \tag{7}$$

ist eine analytische Selbstabbildung $(\sigma \times \tau)$ von $S^m \times PC(n)$ gegeben, die mit φ [s. (1)] vertauschbar ist; $(\sigma \times \tau)$ induziert daher eine analytische Selbstabbildung (σ, τ) von $P(m, n)$. Wir verbinden die Matrix der (in den Variablen x_i bzw. z_j linearen) Abbildung (6) bzw. (7) durch eine stetige Schar reeller orthogonaler Matrizen $0(t)$ bzw. $0'(t)$ mit der Einheitsmatrix. $0(t)$ und $0'(t)$ definieren dann eine Schar mit φ vertauschbarer Selbstabbildungen von $S^m \times PC(n)$ und damit eine Schar von Selbstabbildungen von $P(m, n)$, die mit (σ, τ) beginnt und mit der Identität endet. (σ, τ) ist also in die Identität deformierbar und induziert daher den identischen Automorphismus der Homologiegruppe $H(m, n)$.

Um den Schnitt $[C_i, D_j] \circ [C_{i'}, D_{j'}]$ zu bestimmen, betrachten wir die Permutationen

$$\begin{cases} \sigma\colon\ i' + \mu \to i + 1 - \mu; \\ \tau\colon\ j' + \nu \to j + 1 - \nu, \quad \mu = 0, 1, \ldots, m, \quad \nu = 0, 1, \ldots, n. \end{cases} \tag{8}$$

(Falls die in (8) auftretenden Zahlen nicht im Intervall $[0, m]$ bzw. $[0, n]$ liegen, sind sie mod $m+1$ bzw. mod $n+1$ abzuändern.)

Die Mannigfaltigkeit $(\sigma \times \tau)(S^{i'} \times PC(j'))$ wird durch die Gleichungen $x_{i+1-\mu} = 0$, $z_{j+1-\nu} = 0$, $\mu = 1, 2, \ldots, m - i'$, $\nu = 1, 2, \ldots, n - j'$, beschrieben. Sie befindet sich relativ zu $S^i \times PC(j)$ in allgemeiner Lage (im Sinne von [1], Ch. VIII, § 2, Nr. 11) und ihr Durchschnitt mit $S^i \times PC(j)$ ist durch $x_{i+i'-m+1} = x_{i+i'-m+2} = \cdots = x_m = 0$, $z_{j+j'-n+1} = z_{j+j'-n+2} = \cdots = z_n = 0$, gegeben, d.h.

$$(\sigma \times \tau)(S^{i'} \times PC(j')) \cap S^i \times PC(j) = \begin{cases} S^{i+i'-m} \times PC(j + j' - n) & \text{für } i + i' \geqq m,\ j + j' \geqq n \\ \emptyset & \text{sonst.} \end{cases}$$

Da Φ eine analytische Überlagerung ist, befindet sich auch $(\sigma, \tau)(P(i', j'))$ in allgemeiner Lage relativ zu $P(i, j)$, und es ist

$$(\sigma, \tau)(P(i', j')) \cap P(i, j) = \begin{cases} P(i + i' - m, j + j' - n) & \text{für } i + i' \geqq m,\ j + j' \geqq n \\ \emptyset & \text{sonst.} \end{cases}$$

Für den Schnitt ihrer Homologieklassen gilt daher (s. [1], Ch. VIII, § 2, Nr. 11)

$$(9)\qquad [C_{i'}, D_{j'}] \circ [C_i, D_j] = \begin{cases} [C_{i+i'-m}, D_{j+j'-n}] & \text{für } i+i' \geqq m,\ j+j' \geqq n \\ 0 & \text{sonst.} \end{cases}$$

Durch Übergang zum Dualen erhalten wir nun aus (9) die multiplikative Struktur des Kohomologieringes $H^*(m, n)$. Der Wert der zu $[C_{m-i}, D_{n-j}]$ dualen Kohomologieklasse $\Delta[C_{m-i}, D_{n-j}]$ auf $[C_\mu, D_\nu]$, $i, \mu = 0, 1, \ldots, m$, $j, \nu = 0, 1, \ldots, n$, ist gleich der Schnittzahl von $[C_\mu, D_\nu]$ mit $[C_{m-i}, D_{n-j}]$ ($=0$ für $\mu + 2\nu \neq i + 2j$). Daher folgt aus (5) und (9)

$$(10)\qquad \Delta[C_{m-i}, D_{n-j}] = (c^i, d^j), \quad i = 0, 1, \ldots, m,\ j = 0, 1, \ldots, n.$$

Satz 1. *Der Kohomologiering* mod 2 *von* $P(m, n)$, $H^*(m, n)$, *wird von den 1- bzw. 2-dimensionalen Klassen* $c = (c^1, d^0)$ *und* $d = (c^0, d^1)$ [s. (5)] *erzeugt. Es bestehen die definierenden Relationen* $c^{m+1} = 0$, $d^{n+1} = 0$.

Bezeichnen c' *und* d' *die entsprechend definierten Erzeugenden von* $H^*(m', n')$, *ist* $m' \leqq m$, $n' \leqq n$ *und* $f^*: H^*(m, n) \to H^*(m', n')$ *der durch die Injektion* $P(m', n') \to P(m, n)$ (s. D) *induzierte Homomorphismus, so gilt* $f^*(c) = c'$, $f^*(d) = d'$.

Der erste Teil von Satz 1 folgt aus (9) und (10), weil beim Übergang zum Dualen, Δ, die Schnittbildung in $H(m, n)$ in das $\cup$-Produkt in $H^*(m, n)$ übergeht.

Für den zweiten Teil hat man zu beachten, daß $P(m', n')$ nichts anderes ist als die Vereinigung derjenigen Zellen (C_i, D_j) (s. B) von $P(m, n)$, für die $i \leqq m'$ und $j \leqq n'$ ist; die Behauptung folgt dann aus der Definition von c, c', d, d'.

Bemerkung. Satz 1 läßt sich auch mit Hilfe der spektralen Kohomologiefolge des Faserraums $\{P(m, n), p, PR(m), PC(n), Z_2\}$ (s. A) gewinnen: Man kann die Kohomologie von Basis und Faser als bekannt voraussetzen. Es läßt sich unschwer zeigen, daß die spektrale Kohomologiefolge mod 2 von $P(m, n)$ trivial ist, d.h. daß die Faser mod 2 total nicht nullhomolog ist (s. [2], Chap. III, 7). Dann erhält man die Struktur von $H^*(m, n)$ vermöge [2], Chap. III, Prop. 9.

E. Die „squares" in $P(m, n)$. Die STEENRODschen Sq^i-Kohomologieoperationen[3]) in $H^*(m, n)$ können wegen Satz 1 und wegen der CARTANschen Produktformel $Sq^i(xy) = \sum_{\nu+\mu=i} Sq^\nu x\, Sq^\mu y$ durch die $Sq^\nu c$ und $Sq^\nu d$ ausgedrückt werden. Es gilt

$$(11)\qquad Sq^0 c = c,\quad Sq^1 c = c^2,\quad Sq^i c = 0 \qquad \text{für } i > 1.$$

$$(12)\qquad Sq^0 d = d,\quad Sq^1 d = cd,\quad Sq^2 d = d^2,\quad Sq^j d = 0 \qquad \text{für } j > 2.$$

Während der Kohomologiering mod 2 von $P(m, n)$ nach Satz 1 mit dem von $PR(m) \times PC(n)$ übereinstimmt, fallen die Sq^i nach (12) verschieden aus:

[3]) Mit Sq^i bezeichnen wir diejenige „square"-Operation, mod 2 (s. [4] oder [5]), die die Dimension um i erhöht.

In $PR(m) \times PC(n)$ ist $Sq^1 x = 0$ für jede 2-dimensionale Kohomologieklasse x, in $P(m, n)$ ist $Sq^1 d = cd \neq 0$ für $m, n \geqq 1$. Diese Gleichung, $Sq^1 d = cd$, ist die einzige unter den Gln. (11) und (12), die wir beweisen müssen; die anderen sind bekannt (s. [4] oder [5]). Die Kohomologieoperation Sq^1 in $H^*(m, n)$ ist nach [5], Nr. 3 und 4 der zur exakten Folge $0 \to Z_2 \xrightarrow{2} Z_4 \to Z_2 \to 0$ gehörige BOCKSTEIN-Homomorphismus δ^*: $H^*(m, n) \to H^*(m, n)$; Z_r bezeichnet die zyklische Gruppe der Ordnung r. Nach (4) ist $\partial(C_1, D_1) = 2(C_0, D_1)$, $m \geqq 1$, $n \geqq 1$, und im Rand anderer Zellen als (C_1, D_1) kommt (C_0, D_1) nicht vor. Daraus folgt: $\delta^*(c^0, d^1) = (c^1, d^1)$ [s. (5)], d.h. aber $Sq^1 d = (c^1, d^1) = cd$, letzteres wegen (9) und (10). Diese Gleichung ist auch noch richtig für $m = 0$ oder $n = 0$; beide Seiten sind dann 0 [für $m = 0$, weil dann $H^3(m, n)$ trivial ist].

F. Die STIEFEL-WHITNEYsche Klasse von $P(m, n)$. Ist $\mathfrak{B} = \{B, p, P, S^{r-1}, 0_r\}$ ein Faserraum mit einem Polyeder P als Basis, der $(r-1)$-Sphäre als Faser und der orthogonalen Gruppe 0_r als Strukturgruppe, so bezeichnet $W_j(\mathfrak{B})$ die mod 2 reduzierte j-te STIEFEL-WHITNEYsche Klasse von $\mathfrak{B}$, $j = 0, 1, \ldots, r$ (s. [3], § 38). $W(\mathfrak{B}) = \sum_{j=0}^{r} W_j(\mathfrak{B})$ bezeichnen wir als die STIEFEL-WHITNEYsche Klasse von $\mathfrak{B}$ schlechthin.

Ist insbesondere $P = P(m, n)$ (s. A) und $\mathfrak{B}$ der Faserraum der Tangenteneinheitsvektoren (bezüglich irgendeiner RIEMANNschen Metrik) so schreiben wir $W_j(m, n)$ statt $W_j(\mathfrak{B})$ und $W(m, n)$ statt $W(\mathfrak{B})$.

Satz 2. *Die* STIEFEL-WHITNEY*sche Klasse von $P(m, n)$ ist gegeben durch*

$$W(m, n) = (1 + c)^m (1 + c + d)^{n+1}.$$ [4])

[*Definition von $P(m, n)$ s.* A, *von c und d s. Satz 1.*]

Beweis durch Induktion nach m und n: Satz 2 ist richtig für $m = n = 0$. Sei nun $m > 0$ oder $n > 0$.

Für $n > 0$ ist $P(m, n-1)$ bezüglich der in D definierten Injektion eine analytische Untermannigfaltigkeit von $P(m, n)$ und repräsentiert die Homologieklasse $[C_m, D_{n-1}] \in H(m, n)$. Die hierzu duale Kohomologieklasse ist $d = (c^0, d^1)$ [s. (10)]. N sei der Faserraum der zu $P(m, n-1)$ normalen Einheitsvektoren von $P(m, n)$. Nach THOM (s. [7] oder [9], Chap. III, Nr. II) gilt

$$\psi^*(W_j(N)) = Sq^j d. \tag{13}$$

Dabei ist ψ^*: $H^*(m, n-1) \to H^*(m, n)$ der zur Injektion $P(m, n-1) \to P(m, n)$ gehörige „Umkehrhomomorphismus"; er genügt der Beziehung (s. [9], Introduct. VI)

$$\psi^*(f^*(y)) = y\, d, \quad y \in H^*(m, n); \tag{14}$$

[4]) Den Satz 2 und damit einen gegenüber dem ursprünglichen erheblich vereinfachten Beweis von Satz 3 verdanke ich Herrn D. PUPPE, der $W(m, n)$ mit der Methode von WU [12] berechnet hat.

$f^*\colon H^*(m, n) \to H^*(m, n-1)$ der durch die Injektion induzierte Homomorphismus.

f^* ist eine Abbildung *auf* (Satz 1); wir wählen $W_i \in H^*(m, n)$ so, daß $f^*(W_i) = W_i(N)$ ist. Aus (13) und (14) folgt dann $W_i d = Sq^i d$. Hieraus und aus (12) $W_0 \equiv 1$, $W_1 \equiv c$, $W_2 \equiv d \bmod d^n$ und somit

$$W(N) = f^*(1 + c + d). \tag{15}$$

Ist T der Faserraum der Tangenteneinheitsvektoren von $P(m, n)$, T' der über $P(m, n-1)$ gelegene Teil von T, so gilt (s. [3], 35.7)

$$W(T') = f^* W(T) = f^* W(m, n). \tag{16}$$

Nach der Whitneyschen Dualitätsformel (s. [11], § 3) ist

$$W(T') = W(m, n-1)\, W(N). \tag{17}$$

Die Induktionsvoraussetzung über $W(m, n-1)$ besagt wegen Satz 1

$$W(m, n-1) = f^*\big((1 + c)^m (1 + c + d)^n\big). \tag{18}$$

Einsetzen von (15), (16) und (18) in (17) ergibt

$$f^* W(m, n) = f^*\big((1 + c)^m (1 + c + d)^{n+1}\big),$$

d.h.

$$W(m, n) \equiv (1 + c)^m (1 + c + d)^{n+1} \bmod d^n. \tag{19}$$

Diese Formel ist trivialerweise auch richtig für $n = 0$.

Als Zweites betrachten wir die Injektion $P(m-1, n) \to P(m, n)$, falls $m > 0$. $P(m-1, n)$ repräsentiert die Homologieklasse $[C_{m-1}, D_n] \in H(m, n)$ (s. D); hierzu dual ist die Kohomologieklasse $c = (c^1, d^0)$ [s. (10)]. Eine zur vorangehenden genau analoge Betrachtung ergibt nun

$$W(M) = f^*(1 + c) \tag{15'}$$

und

$$W(m, n) \equiv (1 + c)^m (1 + c + d)^{n+1} \bmod c^m. \tag{19'}$$

Dabei bezeichnet $f^*\colon H^*(m, n) \to H^*(m-1, n)$ wieder den durch die Injektion induzierten Homomorphismus und M ist der Faserraum der auf $P(m-1, n)$ normalen Einheitsvektoren von $P(m, n)$.

Nach (19) und (19') ist $W(m, n) \equiv (1+c)^m (1+c+d)^{n+1} \bmod c^m d^n$. Der homogene Bestandteil vom Grade $m + 2n$ auf der rechten Seite dieser Kongruenz ist $(m+1)(n+1) c^m d^n$. Andererseits ist (s. [3], 39.7) $W_{m+2n}(m,n) = N(m, n) c^m d^n$, wenn $N(m, n)$ die Eulersche Charakteristik von $P(m, n)$ bezeichnet. Der Beweis des Satzes 2 ist also vollendet, wenn wir noch gezeigt haben, daß $N(m, n) \equiv (m+1)(n+1) \bmod 2$ ist. Aus der Struktur von $H^*(m, n)$ (s. Satz 1) ergibt sich aber durch einfache Rechnung

$$N(m, n) = \tfrac{1}{2}\big(1 + (-1)^m\big)(n + 1) \equiv (m + 1)(n + 1) \bmod 2.$$

G. Die Erzeugenden von $\mathfrak{N}$.

Satz 3. *Für jede natürliche Zahl i, die nicht von der Form 2^l-1 ist, seien die ganzen Zahlen r und s durch $i+1=2^r(2s+1)$ erklärt. Es sei*

$$P(i)=\begin{cases} P(i,0)=PR(i) & \text{für gerades } i \\ P(2^r-1, s2^r) & \text{für ungerades } i \text{ (s. A).} \end{cases}$$

$P(i)$ ist eine i-dimensionale kompakte differenzierbare Mannigfaltigkeit; x_i bezeichne ihre Klasse in der Algebra $\mathfrak{N}$ (s. [8], Chap. IV).

$\mathfrak{N}$ kann aufgefaßt werden als Polynomalgebra $K[x_2, x_4, x_5, \ldots]$ in den Variablen x_i, $i=2,4,5,6,8,\ldots$ über dem Primkörper K der Charakteristik 2.

NB. Satz 3 geht nur insofern über das Ergebnis von THOM (s. [8], S. 79ff.) hinaus, als auch für die ungeraden Dimensionen $i>5$ explizit repräsentierende Mannigfaltigkeiten für die Variablen x_i angegeben werden.

Beweis. Es seien $K[\iota]$ der Ring der Polynome über K in den Variablen $t_1, t_2, \ldots, t_\iota$, $S[\iota]<K[\iota]$ die Unteralgebra der symmetrischen Polynome, $S_j(\iota)$ die j-te elementarsymmetrische Funktion der t_ν, $j=0,1,\ldots,\iota$, und $S^h(\iota)=\sum_{\nu=1}^{\iota} t_\nu^h$, $h=0,1,\ldots$.

Für jedes $\iota \geqq i$ definieren wir einen gradtreuen Homomorphismus $\Psi_{i,\iota}$: $S[\iota]\to H^*(i)$ durch

$$\Psi_{i,\iota}(S_j(\iota))=\begin{cases} W_j(i) & \text{für } j\leq i \\ 0 & \text{für } j>i. \end{cases} \tag{20}$$

Dabei bezeichnet $H^*(i)$ den Kohomologiering mod 2 und $W_j(i)$ die j-te STIEFEL-WHITNEYsche Klasse von $P(i)$.

$\Psi_{i,\iota}$ führt $\prod_{\nu=1}^{\iota}(1+t_\nu)=\sum_{\nu=0}^{\iota} S_\nu(\iota)$ in $W(i)=\sum_{\nu=0}^{i} W_\nu(i)$ über und ist unter den gradtreuen Homomorphismen $S[\iota]\to H^*(i)$ dadurch charakterisiert.

Für den Beweis des Satzes 3 genügt es nach [8], Chap. IV, Nr. 7 zu zeigen, daß $\Psi_{i,i}(S^i(i))\neq 0$ ist; wiederum nach [8] können wir uns dabei auf ungerades i beschränken. Wir beweisen nun zunächst die Gleichung

$$\Psi_{i,\iota}(S^h(\iota))=\Psi_{i,i}(S^h(i)), \quad \iota\geq i \tag{21}$$

und zeigen dann $\Psi_{i,i+2}(S^i(i+2))\neq 0$.

Um (21) zu erhalten, definieren wir einen gradtreuen Homomorphismus $\phi_{i,\iota}$: $K[\iota]\to K[i]$ durch $\phi_{i,\iota}(t_\nu)=\begin{cases} t_\nu \text{ für } \nu\leq i \\ 0 \text{ für } \nu>i \end{cases}$. Man bestätigt leicht, daß

$$\phi_{i,\iota}(S_j(\iota))=\begin{cases} S_j(i) & \text{für } j\leq i \\ 0 & \text{für } j>i \end{cases} \tag{22}$$

und

$$\phi_{i,\iota}(S^h(\iota))=S^h(i) \tag{23}$$

ist. Aus (22) und (20) folgt $\Psi_{i,i}\circ\phi_{i,\iota}(S_j(\iota))=\Psi_{i,\iota}(S_j(\iota))$, $j=0,1,\ldots,\iota$, also $\Psi_{\iota,i}\circ(\phi_{i,\iota}|S[\iota])=\Psi_{i,\iota}$. Wendet man auf (23) $\Psi_{i,i}$ an, so folgt hieraus (21).

Für die Berechnung von $\Psi_{i,i+2}(S^i(i+2))$ benötigen wir die Darstellung von $S^h(2)$ als Polynom in $S_1(2)$ und $S_2(2)$. Die bekannte Identität

$$\sum_{j=0}^{\iota} S_j(\iota)\, S^{h-j}(\iota) = 0, \quad h \geqq \iota \tag{24}$$

[Beweis: Das Polynom $\prod_{\nu=1}^{\iota}(1+tt_\nu) - \sum_{j=0}^{\iota} S_j(\iota)\, t^j$ über $K[\iota]$ hat die Nullstellen t_ν^{-1}, $\nu = 1, 2, \ldots, \iota$. Man erhält also, wenn man t_ν^{-1} in dieses Polynom einsetzt und mit t_ν^h multipliziert: $0 = \sum_{j=0}^{\iota} S_j(\iota)\, t_\nu^{h-j}$ und hieraus durch Summation über ν die Gl. (24).]

ergibt für $\iota = 2$

$$S^h(2) = S_1(2)\, S^{h-1}(2) + S_2(2)\, S^{h-2}(2), \quad h \geqq 2. \tag{25}$$

Hieraus folgt durch Induktion nach h

$$S^h(2) = \sum_{p+2q=h} b(p+q-1, q)\, (S_1(2))^p\, (S_2(2))^q, \quad h = 1, 2, \ldots. \tag{26}$$

Dabei ist $b(p+q-1, q)$ der Binomialkoeffizient $\binom{p+q-1}{q} \bmod 2$ ($=1$ für $q=0$, $=0$ für $q<0$ oder $p<q\neq 0$), und es wird über alle nicht negativen ganzen p, q mit $p+2q=h$ summiert.

(26) ist richtig für $h=1, 2$, denn $S^1(2) = S_1(2)$ und $S^2(2) = (S_1(2))^2$. Für $h>2$ ergeben (25) und die Induktionsvoraussetzung

$$\begin{aligned} S^h(2) &= \sum_{p+2q=h-1} b(p+q-1, q)\, (S_1(2))^{p+1}\, (S_2(2))^q + \\ &+ \sum_{p+2q=h-2} b(p+q-1, q)\, (S_1(2))^p\, (S_2(2))^{q+1} \\ &= \sum_{p+2q=h} \big(b(p+q-2, q) + b(p+q-2, q-1)\big)\, ((S_1(2))^p\, (S_2(2))^q \\ &= \sum_{p+2q=h} b(p+q-1, q)\, ((S_1(2))^p\, (S_2(2))^q, \end{aligned}$$

letzteres wegen der bekannten Additionsformel für Binomialkoeffizienten.

Durch die Festsetzungen

$$\left.\begin{aligned} \Psi(t_{2\nu-1} + t_{2\nu}) &= c \\ \Psi(t_{2\nu-1} t_{2\nu}) &= d \\ \Psi(t_{2n+2+\mu}) &= c \end{aligned}\right\} \quad \begin{aligned} &\nu = 1, 2, \ldots, n+1, \quad \mu = 1, 2, \ldots, m, \\ &n = s2^r, \quad m = 2^r - 1 \quad \text{(s. Satz 3)} \end{aligned}$$

definieren wir einen gradtreuen Homomorphismus der von den $(t_{2\nu-1} + t_{2\nu})$, $(t_{2\nu-1} t_{2\nu})$ und $t_{2n+2+\mu}$ erzeugten Unteralgebra von $K[i+2]$ in $H^*(i) = H^*(m, n)$. Ψ führt das Polynom

$$\begin{aligned} \prod_{\varrho=1}^{i+2} (1+t_\varrho) &= \prod_{\nu=1}^{n+1} (1+t_{2\nu-1})\,(1+t_{2\nu}) \prod_{\mu=1}^{m} (1+t_{2n+2+\mu}) \\ &= \prod_{\nu=1}^{n+1} (1 + (t_{2\nu-1} + t_{2\nu}) + t_{2\nu-1} t_{2\nu}) \cdot \prod_{\mu=1}^{m} (1+t_{2n+2+\mu}) \end{aligned}$$

in $(1+c+d)^{n+1}(1+c)^m = W(m,n) = W(i)$ über. Die Einschränkung von Ψ auf $S[i+2]$ stimmt also mit $\Psi_{i,i+2}$ überein. Daher ist

$$\begin{aligned}\Psi_{i,i}\big(S^i(i)\big) &= \Psi_{i,i+2}\big(S^i(i+2)\big) = \Psi\big(S^i(i+2)\big) = \Psi\Big(\sum_{\varrho=1}^{i+2} t_\varrho^i\Big)\\ &= (n+1)\,\Psi(t_1^i + t_2^i) + m\,\Psi(t_{i+2}^i) = (n+1)\,\Psi\big(S^i(2)\big) + m\,\Psi(t_{i+2}^i)\\ &= (n+1)\,\Psi\Big(\sum_{p+2q=i} b(p+q-1,q)\,\big(S_1(2)\big)^p\big(S_2(2)\big)^q\Big) + m\,\Psi(t_{i+2}^i)\\ &= (n+1)\sum_{p+2q=i} b(p+q-1,q)\,c^p d^q + m\,c^i.\end{aligned}$$

Wegen $i > m$ ist $c^i = 0$ (s. Satz 1). Ferner ist $c^p d^q$ für $p+2q=i$ nur dann von 0 verschieden, wenn $p=m$ und $q=n$ ist (Satz 1). Beachtet man noch, daß $n+1 \equiv 1(2)$ ist, so ergibt sich $\Psi_{i,i}\big(S^i(i)\big) = b(m+n-1,n)\,c^m d^n$. Nun ist $m+n-1 = s\,2^r + (2^r-2)$ und $n = s\,2^r$. Daraus geht hervor, daß die dyadische Entwicklung von n in der von $m+n-1$ enthalten ist, d.h. (s. [6], Lemma 2.2), daß $b(m+n-1,n) = 1$ und $\Psi_{i,i}\big(S^i(i)\big) = c^m d^n \neq 0$ ist, w.z.b.w.

Bemerkung. Die in Satz 3 getroffene Auswahl der Erzeugenden von $\mathfrak{N}$ unter den Mannigfaltigkeiten $P(m,n)$ ist nicht eindeutig festgelegt. Aus dem Beweis geht hervor, daß man z.B. in der Dimension 6 auch $P(2,2)$ statt $P(6,0)$ und in der Dimension 9 $P(5,2)$ statt $P(1,4)$ hätte nehmen können.

H. Anwendung auf die Algebra Ω. Für ungerades $i \neq 2^l-1$ ist die Mannigfaltigkeit $P(i)$ (s. Satz 3) orientierbar (s. C). Versehen wir sie mit einer festen Orientierung, so definiert sie ein Element $v_i \in \Omega^i$ (s. Einleitung oder [8], Chap. IV, 1), das beim natürlichen Homomorphismus $\Omega \to \mathfrak{N}$ in x_i übergeht. v_i ist also sicher nicht Null. Es gilt aber: *Die Ordnung von $v_i \in \Omega^i$ ist* 2.

Es gibt nämlich eine differenzierbare, orientierungsumkehrende Involution von $P(i)$. Um dies einzusehen, betrachten wir das Produkt $S^m \times PC(n)$ mit $m = 2^r-1$, $n = s\,2^r$ (s. Satz 3). Ist $x = (x_0, x_1, \ldots, x_m)$ ein Punkt aus S^m, so bezeichne $\tilde{x}$ den Punkt $(x_0, x_1, \ldots, x_{m-1}, -x_m)$ aus S^m. Durch $\tilde{I}(x,z) = (\tilde{x}, z)$, $x \in S^m$, $z \in PC(n)$, definieren wir eine differenzierbare Involution von $S^m \times PC(n)$ vom Grade -1. $\tilde{I}$ ist mit der Deckbewegung φ [s. (1)] vertauschbar und induziert daher eine differenzierbare Involution I von $P(m,n)$; I kann durch die Gleichung $I \circ \Phi = \Phi \circ \tilde{I}$ definiert werden. Φ hat als zweiblättrige Überlagerung den Grad ± 2, also I wegen $I \circ \Phi = \Phi \circ \tilde{I}$ den Grad -1.

Hieraus folgt nun: *Beim natürlichen Homomorphismus $\Omega \to \mathfrak{N}$ ist die von den x_i (s. Satz 3) mit ungeradem $i \neq 2^l-1$ erzeugte Unteralgebra von $\mathfrak{N}$ isomorphes Bild der von den v_i erzeugten Unteralgebra von Ω.* Insbesondere ergibt sich, daß die Gruppen Ω^k nicht zu „klein" sein können; z.B. gilt: *Für $k \geq 8$ ist Ω^k nicht trivial*, d.h. in jeder Dimension $k \geq 8$ gibt es nicht-berandende kompakte orientierbare differenzierbare Mannigfaltigkeiten.

Zum Beweis genügt es (nach dem eben Gesagten und nach [8], Chap. IV, Nr. 8), ein Produkt von Räumen $P(i)$, i ungerade $\neq 2^l-1$, und komplexen projektiven Räumen $PC(2j)$ gerader komplexer Dimension anzugeben, das

die Gesamtdimension k hat; d.h. wir haben eine Partition von k in ungerade natürliche Zahlen $\neq 2^l - 1$ und durch 4 teilbare natürliche Zahlen anzugeben. Für $k \equiv 3\,(4)$, $k \geq 11$, ist $k = 11 + (k - 11)$, für $k \equiv 2\,(4)$, $k \geq 10$, ist $k = 5 + 5 + (k - 10)$ und in allen anderen Fällen ist $k = k$ eine solche Partition.

Literatur

[1] Lefschetz, S.: Topology. Amer. Math. Soc. Colloq. Publ. **12** (1930). — [2] Serre, J. P.: Homologie singulière des espaces fibrés; applications. Ann. of Math. **54**, 425—505 (1951). — [3] Steenrod, N.: The topology of fibre bundles. Princeton Math. Ser. 14. — [4] Steenrod, N.: Products of cocycles and extensions of mappings. Ann. of Math. **48**, 290—320 (1947). — [5] Steenrod, N.: Homology groups of symmetric groups and reduced power operations; cyclic reduced powers of cohomology classes. Proc. Nat. Acad. Sci. U.S.A. **39**, 213—223 (1953). — [6] Steenrod, N., and J. H. C. Whitehead: Vector fields on the n-sphere. Proc. Nat. Acad. Sci. U.S.A. **37**, 58—63 (1951). — [7] Thom, R.: Variétés plongées et i-carrés. C. R. Acad. Sci. Paris **230**, 507—508 (1950). — [8] Thom, R.: Quelques propriétés globales des variétés différentiables. Comment. Math. Helv. **28**, 17—87 (1954). — [9] Thom, R.: Espaces fibrés en sphères et carrés de Steenrod. Ann. Ecole norm. sup. (3) **69**, 109—182 (1952). — [10] Whitehead, J. H. C.: Combinatorial Homotopy. I. Bull. Amer. Math. Soc. **55**, 213—245 (1949). — [11] Wu, Wen-Tsün: On the product of sphere-bundles and the duality theorem mod 2. Ann. of Math. **49**, 641—653 (1948). — [12] Wu, Wen-Tsün: Classes caractéristiques et i-carrés. C. R. Acad. Sci. Paris **230**, 508—511 (1950).

Heidelberg, Mathematisches Institut der Universität

(Eingegangen am 22. November 1955)

NEUMANN, H.
Math. Zeitschr. Bd. 65, S. 36—69 (1956)

On varieties of groups and their associated near-rings

By
HANNA NEUMANN

Introduction

The present paper arose out of the attempt to clarify some questions on varieties of groups and laws in groups. The central theme is the role played by the number of variables involved in laws. For reasons that will appear later, certain near-rings connected with free groups proved a helpful tool. Once introduced, these near-rings raise their own problems. The work done on near-rings by previous authors (cf. e.g. [2], [3]) has very little bearing on those arising here: we have no chain conditions available; but to a certain extent the similarity of our near-rings to ordinary matrix rings makes up for this.

The first part (§§ 1—3) deals with the interrelation between certain varieties of groups. A variety of groups is determined by the set of all laws holding in all groups of the variety or, equivalently, by a fully invariant subgroup V of the free group $F = \{e_1, e_2, \ldots\}$ of countably infinite rank. The intersection V_n of V with the subgroup F_n of F which is generated by $e_1, e_2, \ldots, e_n$, determines in the form F_n/V_n the free group of rank n of the variety. A number of questions arise naturally in this context; for example we may ask for the different varieties of which F_n/V_n is the free group of rank n. Or again, bearing in mind that V_n represents the laws in n variables of the variety determined by V, we enquire into the relation between $V_m = F_m \cap V$ and the set of all laws in m variables that hold in F_n/V_n. The results may be summarized as follows: Every variety, that is every fully invariant subgroup V of F, determines two chains of fully invariant subgroups, one descending and one ascending, both "converging" to V. These two chains are in a sense dual to each other; while the n^{th} term of the ascending chain corresponds to the set of all laws in n variables of the variety, the n^{th} term of the descending chain represents the set of all laws holding in every group of the variety that can be generated by n elements. The group F_n/V_n is the free group of rank n of precisely all those varieties which are determined by fully invariant subgroups of F "between" the n^{th} term of the ascending chain and the n^{th} term of the decending chain. Several of the many unsolved problems on laws in groups are equivalent to the question whether one or the other of these chains becomes stationary after a finite number of steps, or is stationary in certain places.

The situation described here is probably widely known. But while certain aspects of it, and specific examples, can be found in the literature (cf. e.g. [8], [9], [11], [14]), no connected account seems to exist. This is the justification of the first part: what little we use of it in the second part, mainly the significance of the ascending chain, could have been dealt with rather more briefly.

Part II is devoted to the near-rings mentioned before. They are introduced in § 4. We consider a reduced free group G_n of finite or infinite rank n, that is a group which is the free group of rank n of some variety, generated freely by the elements $e_1, e_2, \ldots, e_n$. These generators have the property (characteristic for reduced free groups[1])), that every mapping of them into the group can be continued to an endomorphism of the group. Consequently addition of endomorphisms may be so defined that, together with the usual definition of multiplication, the endomorphisms of G_n form a near-ring Γ_n. The definition of addition differs from that usual for mappings of a group into itself ([2], [15]), with the result that in our near-rings the right distributive law holds, that is a right-hand factor distributes over a sum as left-hand factor, while in the near-ring of all mappings of a group into itself one customarily has the left distributive law[2]).

The representation of an endomorphism by means of its n "components", namely the maps of the free generators, leads to an interpretation of these near-rings as a generalization of matrix rings. In fact if G_n is the free group of an abelian variety, this interpretation coincides with the representation of the ring of endomorphisms as ring of matrices over the integers (or integers modulo m). A matrix ring possesses a module basis consisting of those matrices having 1 in the i^{th} row and j^{th} column and zeros elsewhere. Our near-rings contain corresponding elements; they also form an additive basis, if n is finite. In addition they have the property that they distribute on both sides. This "distributive basis" plays a decisive part. However, the basis property gets lost if n is infinite. For this reason we confine ourselves subsequently to finite and countably infinite rank, and in the latter case restrict ourselves to what may be loosely described as the near-ring of all row- and column-finite matrices (§ 5). This near-ring, denoted by Γ_ω, can be represented as the union of all near-rings Γ_n for finite n and therefore still possesses the basis property. Due to the existence of a "distributive basis", the ideals in the near-rings Γ_n and Γ_ω, defined as normal subgroups of the additive group which are closed under right and left multiplication by elements of the near-ring, are precisely the kernels of the homomorphisms of these near-rings (§ 6). On the other hand, the specific nature of our near-rings permits a different characterization of an ideal, namely as the subset of all those matrices whose components vary over a fixed fully invariant subgroup of the associated reduced free group. This remains true for the restricted near-ring Γ_ω in place of the near-ring of all endomorphisms of the reduced free group G of countably infinite rank; and this is the reason that these near-rings Γ_ω are sufficient for our purposes. This characterization then shows that all near-rings Γ_n and Γ_ω are homomorphic images of the corresponding near-rings Φ_n and Φ_ω associated with the absolutely free groups F_n and F respectively. Next we discuss the formal properties of the

[1]) Cf. [6]; P. Hall uses the term "relatively free group".

[2]) In Zassenhaus however this becomes the right distributive law due to his definition of the product $\alpha\beta$ as the mapping β followed by the mapping α.

lattice of ideals and introduce ideal multiplication (§ 7). The similarity to matrix rings is essential here. Ideal multiplication in the near-ring corresponds in the group to the familiar process of obtaining new fully invariant subgroups by substituting the elements of one for the generators in the words of another fully invariant subgroup. It is this process of substitution in the free group which benefits most by being translated into multiplication in the near-ring. The limitation of the number of variables for which one may substitute in the case of finite rank n then expresses itself in the fact that ideal multiplication in Γ_n is in general not associative. By contrast, ideal multiplication proves associative in the near-rings Γ_ω. In the last two paragraphs we specialize to the near-rings Φ_n and Φ_ω belonging to the absolutely free groups, mainly because we make use of the SCHREIER property that every subgroup of a free group is itself free. The ideals in Φ_ω (§ 8) form a semigroup with right cancellation; in fact more than that, right multiplication by a fixed ideal is an iso-endomorphism of the lattice of ideals. The fully invariant subgroups of F which are fully invariant in a larger fully invariant subgroup of F are just those corresponding to ideal products in Φ_ω. This is no longer true in the case of finite rank n (§ 9): here they correspond merely to the intersections of ideal products in Φ_ω with the near-ring Φ_n. A closer analysis of the situation shows this to be the immediate reason for the non-associativity of ideal multiplication in Φ_n.

In conclusion it should be mentioned that our representation of the endomorphisms of free groups as a near-ring of matrices can be carried through similarly for the free algebras of more general varieties, for example the varieties of loops, or of groupoids. In fact, precisely this has been done by A. ROBINSON—in different language—for the free groupoid on one generator (cf. [13]; compare also the logarithmetics of I. M. H. ETHERINGTON: cf. [4] and the literature there quoted). ROBINSON states (loc. cit. p. 117) that there is no "natural" definition of multiplication in terms of addition in the case of more than one generator. However, our definition of multiplication of n-rowed "matrices" will do just that also in the case of a free groupoid on n generators.

Part I

1. Preliminaries and notation

We begin with a summary of definitions and facts that will be used throughout, introducing at the same time the notation employed.

All groups will be written additively, the neutral element zero will be denoted by 0 in every group. Capital Roman letters signify groups, small Roman letters denote elements of groups. Small Greek letters stand for endomorphisms of groups. We write $2x$ for $x+x$, generally $nx = x+x+\cdots$, where the sum has n terms; $[x, y]$ denotes the commutator of x and y, $[x, y] = x-y+x+y$; $[x, y, z]$ is the left-normed commutator, $[x, y, z] = [[x, y], z]$.

The free group on $\aleph_0$ generators $e_1, e_2, \ldots$ is denoted by F, the subgroup generated by $e_1, e_2, \ldots, e_n$, for every finite n, is denoted by F_n. Then $F = \bigcup_n F_n$.

F_n may be obtained from F by means of the retractive homomorphism ε_n defined by $e_i\varepsilon_n = e_i$ for $i = 1, \ldots, n$ and $e_i\varepsilon_n = 0$ for $i > n$. Then $F_n = F\varepsilon_n \cong F/F_n^*$, where F_n^*, the kernel of the homomorphism, is the normal closure in F of the free factor generated by $e_{n+1}, e_{n+2}, \ldots$.

1.01. *An element w of F belongs to F_n if, and only if, $w\varepsilon_n = w$. If V is a fully invariant subgroup of F, its intersection V_n with F_n is given by $V_n = V \cap F_n = V\varepsilon_n$. V_n is a fully invariant subgroup of F_n, and $V = \bigcup_n V_n$.*

A *variety of groups* is the class of all groups satisfying a given set of laws (or identical relations). Here a law is a word $v(x_1, x_2, \ldots)$ in the variables x_i; the law holds in the group H if for every substitution of elements $h_1, h_2, \ldots$ of H for the variables $x_1, x_2, \ldots$ one has $v(h_1, h_2, \ldots) = 0$ qua element of H. If $v(x_1, x_2, \ldots)$ varies over the set of all laws satisfied by the groups of the variety, the corresponding words $v(e_1, e_2, \ldots)$ form a fully invariant subgroup V of F. We say: V represents the laws of the variety, the variety corresponds to, or is determined by, the fully invariant subgroup V of F. Every fully invariant subgroup V of F determines a variety:

1.02. *A group H belongs to the variety determined by V if, and only if, every countable subgroup of H is a homomorphic image of F/V. If in particular H can be generated by n elements, then H is a homomorphic image of F_n/V_n.*

Since a variety is determined by all its countable groups, we shall henceforth consider countable groups only.

1.03. *The free groups of rank $\aleph_0$ and n respectively of the variety determined by V are given by $G \cong F/V$ and $G_n \cong F_n/V_n$.*

The letters G and G_n will be reserved for *reduced free groups*, that is groups which are the free groups of some variety.

1.04. *A group is reduced free if, and only if, it possesses a set of generators whose every mapping into the group can be continued to an endomorphism of the group.*

Such a set of generators is called a set of free generators (or canonical generators; cf. [6]). In particular, the maps of the generators e_i of F (or F_n) under the natural homomorphism of F (or F_n) onto G (or G_n) according to 1.03 form a set of free generators of G (or G_n).

We use the following terminology:

1.05. Definition. *For any group H, the variety defined by H is the variety corresponding to the set of all laws that hold in H.*

As H is countable, it may be represented as a factor group of F, $H \cong F/R$; if H can be generated by n elements, then also $H \cong F_n/R_n$. Here R, R_n are not, in general, uniquely determined by H; but in both cases the greatest fully invariant subgroup of F or F_n contained in R or R_n respectively depends only on H. One has (cf. [11]):

1.06. *The variety defined by H is the variety corresponding to the greatest fully invariant subgroup V of F contained in R. The set of all laws of H involving*

at most n variables is given by $V_n = V \cap F_n$. *If* $H \cong F_n/R_n$ *for some normal subgroup* R_n *of* F_n, *then* V_n *is the greatest fully invariant subgroup of* F_n *contained in* R_n.

Different groups may, of course, define the same variety. The variety corresponding to V is, trivially, the variety defined by F/V.

For any set of elements of F (or F_n), the least fully invariant subgroup of F (or F_n) containing the set is called the *fully invariant closure in* F (or *in* F_n) of the given set of elements. It is obtained by forming the closure of the set with respect to the operations of addition, and of substitution of arbitrary elements of F (or F_n) for the generators. The set of elements is referred to as a *basis for* V *in* F (or *for* V_n *in* F_n).

2. The ascending chain determined by a variety

Our object is to examine the relation between the fully invariant subgroups of the groups F_n of finite rank and those of the group F of infinite rank.

2.01. Definition. *If* V_m *is a fully invariant sugbroup of* F_m, *the extension of* V_m *to* F_n $(n > m)$, *or to* F, *is the fully invariant closure of* V_m *in* F_n, *or in* F, *respectively.*

If V, *or* V_n, *is a fully invariant subgroup of* F, *or* F_n, *the restriction of* V, *or* V_n, *to* F_m *is the intersection* $V \cap F_m$, *or* $V_n \cap F_m$, *respectively.*

These two processes of extension and restriction are not in general inverse to each other. While an extension followed by restriction of the result to the previous "level" leads back to the original fully invariant subgroup, this is not always true if the processes are carried out in reverse order.

We first note some obvious facts:

2.02. *If* $l < m < n$, *extending* V_l *first to* F_m, *then extending the result to* F_n, *amounts to the same as extending* V_l *to* F_n. *The same is true with* F *in place of* F_n.

2.03. *The extension of* V_m *to* F *is the union of the extensions of* V_m *to* F_n *for* $n = m+1, m+2, \ldots$.

Corresponding to 2.02 we have trivially:

2.04. *If* $l < m < n$, *restricting* V_n *first to* F_m, *then restricting the result to* F_l, *amounts to the same as restricting* V_n *to* F_l. *The same is true with* F *in place of* F_n.

2.05. *If* V_n *is a fully invariant subgroup of* F_n, $V^{(n)}$ *its extension to* F, *then* $V^{(n)} \cap F_n = V_n$.

Proof. Clearly $V_n \leqq V^{(n)} \cap F_n$. To prove the reverse inclusion, let v be an arbitrary element of $V^{(n)}$ that belongs to F_n. As $V^{(n)}$ is the fully invariant closure of V_n in F, the element v is of the form

$$v = \sum_i v_i(x_{i,1}, \ldots, x_{i,n}),$$

where $v_i(e_1, \ldots, e_n) \in V_n$, and the $x_{i,j}$ are elements of F, that is representable as words $x_{i,j} = x_{i,j}(e_1, e_2, \ldots, e_{k(i,j)})$. But $v \in F_n$, hence $v = v\varepsilon_n$; therefore

$$v = v\varepsilon_n = \sum_i v_i(x_{i,1}\varepsilon_n, \ldots, x_{i,n}\varepsilon_n).$$

But $x_{i,j}\varepsilon_n$ lies in F_n for all i and j, and so each term of this sum belongs to V_n, that is $v \in V_n$.

2.05 combined with 2.02 and 2.04 gives at once:

2.06. *If $l < m < n$, extending V_l to F_n, then restricting the result to F_m, amounts to the same as extending V_l to F_m. The same is true with F in place of F_n.*

We now examine the result of restricting first, and then extending. In this context the following notation will be used throughout the paper:

Notation. If V is a fully invariant subgroup of F, then V_n denotes its restriction to F_n, $V_n = V \cap F_n$; and $V^{(n)}$ is the extension of V_n to F.

Since $V_n \subseteq V \cap F_{n+1} = V_{n+1}$, it follows that $V^{(n)} \subseteq V^{(n+1)}$ for all n. Moreover, as V is the union of its restrictions V_n for all n, V is a fortiori the union of the groups $V^{(n)}$ for all n. Therefore:

2.07. *The fully invariant subgroups $V^{(n)}$ $(n = 1, 2, \ldots)$ of F determined by V form an ascending chain, and V is the union of its terms;*

$$V^{(1)} \subseteq V^{(2)} \subseteq \cdots \subseteq V^{(n)} \subseteq \cdots \subseteq V; \qquad V = \bigcup_n V^{(n)}.$$

The fact that $V^{(1)}$ is the trivial group whenever V is contained in the derived group of F shows that the inclusion may be proper for some terms. We shall give a less trivial example at the end of the paragraph. The significance of the chain is explained by:

2.08. Theorem. *The ascending chain determined by V is finite, i.e. it becomes stationary after a finite number of steps if, and only if, V possesses a basis whose members involve only a finite number of generators. If k is the least integer such that V is the closure of a set of words each of which involves at most k generators, then*

$$V^{(k-1)} \subset V^{(k)} = V^{(k+1)} = \cdots = V.$$

Corollary. *If V is finitely based, the ascending chain is finite.*

Proof. If for some n, $V^{(n)} = V$, then V is the closure of V_n in F, that is, it possesses a basis involving at most $e_1, \ldots, e_n$; thus $n \geq k$. Conversely, if the words $v_i(e_1, \ldots, e_{n(i)})$ with $n(i) \leq k$ form a basis of V, then V is the closure of V_k in F, as the basis elements all belong to F_k, hence to V_k.

The premise of the corollary touches upon a central unsolved problem, namely the question whether every fully invariant subgroup of F is finitely based, or equivalently, whether the ascending chain condition for fully invariant subgroups holds in F. We cannot even state the converse of the corollary, for it is not known either, whether every fully invariant subgroup of a free group of finite rank is finitely based. If V represents the set of all laws of a finite group, then all factor groups F_n/V_n are finite (cf. [11]), hence by SCHREIER's Theorem V_n as free subgroup of F_n is of finite rank, hence it is certainly finitely based. Therefore we have in that case:

2.09. *If V represents the set of laws of a finite group, the ascending chain is finite if, and only if, V is finitely based.*

Again it is not known, whether there exists a finite group whose laws are not finitely based. R. C. LYNDON [9] has shown that the set of all laws of every finite nilpotent group is finitely based.

Finally we determine the restrictions of the terms of the chain:

2.10. Theorem. *If k is defined as in* 2.08, *then*

$$\begin{aligned} V^{(n)} \cap F_m &= V \cap F_m = V_m, && \text{if } n \geq m, \\ V^{(n)} \cap F_m &= V_m, && \text{if } k \leq n < m, \\ V^{(n)} \cap F_m &\subset V_m, && \text{if } n < k \leq m. \end{aligned}$$

Proof. By 2.05, $V^{(m)} \cap F_m = V_m$; also by the definition of V_m, $V \cap F_m = V_m$. If $n \geq m$, then $V^{(m)} \subseteq V^{(n)} \subseteq V$, hense also $V^{(n)} \cap F_m = V_m$.

Next, $k \leq n < m$ implies $V^{(k)} = V^{(n)} = V^{(m)}$, by definition of k; hence $V^{(n)} \cap F_m = V^{(m)} \cap F_m = V_m$.

Finally, $n < k \leq m$ implies $V^{(n)} \subseteq V^{(k-1)} \subset V^{(k)} = V^{(m)}$; hence $V^{(n)} \cap F_m \subseteq V^{(m)} \cap F_m = V_m$. By 2.06, $V^{(n)} \cap F_m$ is the extension of V_n to F_m, therefore, by 2.02, the extension of $V^{(n)} \cap F_m$ to F is $V^{(n)}$. If now we had $V^{(n)} \cap F_m = V_m$, then $V^{(n)} = V^{(m)}$ would follow, since the extension of V_m to F is $V^{(m)}$. Hence $V^{(n)} \cap F_m \subset V_m$.

We conclude the paragraph with an illustration:

2.11. Example. We consider the second derived group of F, which we denote by A for the present[3]). Thus A is seen to be the closure in F of the word $[[e_1, e_2], [e_3, e_4]]$, and therefore $k \leq 4$. Although $k = 4$ is plausible, we know at present only:

$$A^{(1)} = \{0\} \subset A^{(2)} \subseteq A^{(3)} \subseteq A^{(4)} = A.$$

The restriction of every term except the first to the free group F_2 is, by 2.10, the same group, namely the second derived group of F_2. For the restrictions to the free group F_3 one has similarly:

$$A^{(2)} \cap F_3 \subseteq A^{(3)} \cap F_3 = A \cap F_3.$$

The last term is the second derived group of the group F_3; the first is, by 2.06, the extension of the two-variable second derived group to the group F_3. To show that the inclusion here is, in fact, proper, one has to construct a group generated by three elements, which is not metabelian, while any two of its elements generate a metabelian subgroup. An example of such a group exists[4]); therefore

$$A^{(2)} \cap F_3 \subset A^{(3)} \cap F_3, \quad \text{hence} \quad A^{(2)} \subset A^{(3)},$$

the latter by 2.05 and 2.06.

One more application of 2.10 shows that the restriction of the terms of the chain to the free group F_4 are:

$$A^{(2)} \cap F_4 \subset A^{(3)} \cap F_4 \subseteq A^{(4)} \cap F_4 = A \cap F_4.$$

[3]) Neither the notation F^2, nor D_2 or D^2 is convenient in this context.

[4]) The construction of such groups is the subject of a note by B. H. NEUMANN to be published in Proc. Glasgow Math. Ass. **3** (1956).

As before, also the second inclusion is proper, because there exists a non-metabelian group generated by four elements, all whose three-generator subgroups are metabelian[4]). Hence again:

$$A^{(3)} \cap F_4 < A^{(4)} \cap F_4, \quad \text{and so} \quad A^{(3)} < A^{(4)}.$$

We sum up the situation in this example:

2.12. *If A is the second derived group of F, then*

$$\{0\} = A^{(1)} < A^{(2)} < A^{(3)} < A^{(4)} = A, \quad \text{and so } k = 4.$$

That is: the two-variable metabelian laws form a proper subset of the three-variable metabelian laws, and the three-variable metabelian laws form a proper subset of all metabelian laws.

Since the three corresponding fully invariant subgroups of F all have the same intersection with the group F_2, we see incidentally:

2.13. *The free metabelian group of rank 2 is the free group of rank 2 of at least three different varieties of groups.*

We return once more to the finite basis problem. If there are fully invariant subgroups of F which are infinitely based, then a group like $A^{(2)}$, representing the two-variable metabelian laws, might be thought to provide an example: it is defined as the closure in F of all second commutators of the form $[[x(e_1, e_2), y(e_1, e_2)], [z(e_1, e_2), t(e_1, e_2)]]$. However, GRAHAM HIGMAN has shown[5]), that all two-variable metabelian laws follow from the single law $[[x, y], [-x, y]]$, and so the group $A^{(2)}$ is finitely based.

3. The descending chain determined by a variety

We consider again a fixed variety, given by the fully invariant subgroup V of F. Its free groups of finite rank are $G_n \cong F_n/V_n$, where V_n represents all laws of the variety which involve at most n variables. This time we ask for the variety defined by G_n in the sense of 1.05, that is we want to obtain the set of all laws that hold in G_n, as well as the sets of all laws in m variables that hold in G_n. By 1.06, we obtain all the laws of G_n by representing G_n as a factor group of F. We first note:

3.01. *The set of all the laws of $G_n \cong F_n/V_n$ includes the laws given by V.*

For $F_n/V_n = F_n/(F_n \cap V) \cong \{F_n, V\}/V$; this represents F_n/V_n as a subgroup of F/V, and all the laws of a group hold a fortiori in every subgroup of that group.

To represent F_n/V_n as a factor group of F/V, we use the retraction ε_n of F onto F_n, whose kernel is F_n^* (cf. § 1). As V_n is normal (even fully invariant) in $F_n \cong F/F_n^*$, the group $\{V_n, F_n^*\}$ is normal in F and contains F_n^*. Therefore:

3.02. $$F_n/V_n \cong F/\{V_n, F_n^*\},$$

where the isomorphism is that naturally induced by the mapping ε_n of F onto F_n.

---

[5]) Unpublished.

In particular:

3.03. *An element $w(e_1, \ldots, e_n)$ of F belongs to $\{V_n, F_n^*\}$, if and only if, qua element of F_n it belongs to V_n.*

From 3.01 and 3.02 we have: $V \subset \{V_n, F_n^*\}$, hence $\{V, F_n^*\} \subseteq \{V_n, F_n^*\}$. Since the reverse inclusion holds trivially, we obtain

3.04. *For every n, $\{V_n, F_n^*\} = \{V, F_n^*\}$, and $F_n/V_n \cong F/\{V, F_n^*\}$.*

Now the set of all the laws that hold in F_n/V_n is given by the greatest fully invariant subgroup of F contained in $\{V, F_n^*\}$.

Notation. The greatest fully invariant subgroup of F contained in $\{V, F_n^*\}$ is denoted by W^n.

Then $V \subseteq W^n$; moreover, as $F_n^* \supset F_{n+1}^*$, also $\{V, F_n^*\} \supseteq \{V, F_{n+1}^*\}$, and so $W^n \supseteq W^{n+1}$. We now have:

3.05. Theorem. *If W^n is the fully invariant subgroup of F representing the set of all laws that hold in the free group of rank n of the variety determined by V, then the groups W^n for $n = 1, 2, \ldots$ form a descending chain, whose intersection is V,*

$$W^1 \supseteq W^2 \supseteq \cdots \supseteq W^n \supseteq \cdots \supseteq V, \quad \text{and} \quad V = \bigcap_n W^n.$$

Proof. Only the assertion that the chain contracts to V remains to be proved. Since $V \subseteq W^n \subseteq \{V, F_n^*\}$ for every n, it suffices to prove that

$$\bigcap_n \{V, F_n^*\} = V.$$

Trivially, V is contained in the intersection. Now let w be an element of F that does not belong to V. There exists an integer m such that w belongs to the subgroup F_m of F; since $w \notin V$, it follows that $w \notin V_m$, hence by 3.03 and 3.04, $w \notin \{V, F_m^*\}$, and so $w \notin \bigcap_n \{V, F_n^*\}$, as was to be shown.

3.06. Theorem. *The set of all laws in at most m variables that hold in the free group of rank n of the variety determined by V is given by $W^n \cap F_m$,*

$$\begin{aligned} &\textit{where} \quad && W^n \cap F_m = V_m \quad \textit{if} \quad m \leq n, \\ &\textit{and} \quad && W^n \cap F_m \supseteq V_m \quad \textit{if} \quad m > n. \end{aligned}$$

Proof. By 3.03, $W^n \cap F_n = V_n$; hence for $m \leq n$:

$$W^n \cap F_m = W^n \cap F_n \cap F_m = V_n \cap F_m = V_m.$$

If $m > n$, $W^n \supseteq W^m$, hence $W^n \cap F_m \supseteq W^m \cap F_m = V_m$.

It is seen again from the case $n = 1$, that some of the inclusions in Theorem 3.05, and therefore also in Theorem 3.06, may be proper: W^1 always contains the whole derived group of F, and its intersections with the groups F_m therefore always contain the whole derived group of the latter. Again, we shall mention a less trivial example at the end of this paragraph.

Combining 3.05 and 3.06 with the results 2.08 and 2.10 of the last paragraph, we now find:

3.07. Theorem. *If G_n is a reduced free group of finite rank n, $G_n \cong F_n/V_n$, then G_n is the free group of rank n of precisely all those varieties determined by fully invariant subgroups U of F which satisfy $V^{(n)} \subseteq U \subseteq W^n$. In particular, the*

varieties determined by $V^{(n)}$ *and* W^n *are the unique greatest and least varieties respectively of which* G_n *is the free group of rank* n.

Proof. As $V^{(n)} \cap F_n = W^n \cap F_n = V_n$, G_n is the free group of rank n of the varieties corresponding to $V^{(n)}$ and W^n, and therefore of every variety between the two.

Conversely, if the fully invariant subgroup U of F determines a variety of which G_n is the free group of rank n, then $U \cap F_n = V_n$, that is V_n is contained in U, and so the closure $V^{(n)}$ of V_n also is contained in U. On the other hand, G_n is a group of the variety determined by U, hence all the laws represented by U hold in G_n, and so U is contained in the fully invariant subgroup representing all the laws of G_n, that is in W^n. This completes the proof.

A different characterization of the terms of the descending chain will show the "duality" between the ascending and the decending chains associated with the fully invariant subgroup V of F.

3.08. Theorem. *The* n^{th} *term* W^n *of the descending chain associated with* V *represents the set of all those laws that hold in every group of the variety determined by* V *which can be generated by* n *elements.*

Proof. For the proof we denote by U the set of all the laws holding in every n-generator group of the variety determined by V. Since every n-generator group of this variety is a homomorphic map of F_n/V_n, all the laws of F_n/V_n hold in every one of them; hence $W^n \subseteq U$. Conversely, F_n/V_n itself is an n-generator group of the variety, and the set of all its laws is precisely W^n; hence $U \subseteq W^n$, and so $U = W^n$ follows.

Theorem 3.08 is really no more than a restatement of the definition of W^n. The following characterization of W^n is related, but more useful:

3.09. Theorem. *If* H *is any group defining the variety determined by* V, *that is,* V *represents all the laws holding in* H, *then* W^n *represents the set of all those laws that hold in every subgroup of* H *which can be generated by* n *elements.*

Proof. Again we denote by U the set of all laws holding in every n-generator subgroup of H. With H also every subgroup of H is a group of the variety; 3.08 shows therefore that the laws given by W^n hold in every n-generator subgroup of H, hence $W^n \subseteq U$. For the converse, we represent H in the form $H \cong F/R$; then V is the greatest fully invariant subgroup of F contained in R. The subgroup of F/R generated by the n elements $e_1 + R, \ldots, e_n + R$ is $\{F_n, R\}/R \cong F_n/R_n$, where $R_n = F_n \cap R$, and V_n is the greatest fully invariant subgroup of F_n contained in R_n. We show that the sets of all the laws of F_n/V_n and of F_n/R_n are the same. Since F_n/R_n is a homomorphic map of F_n/V_n, every law of the latter holds in the former group. But on the other hand, F_n/V_n can be represented as subgroup of a direct power of F_n/R_n (cf. [*11*]), and every law of a group also holds in every direct power of this group, and therefore also in every subgroup of its direct powers. Thus the laws of F_n/R_n hold in F_n/V_n, and so the two groups possess the same set of laws. But this set of laws is given by W^n, therefore $U \subseteq W^n$, since the laws given by U hold in every n-generator subgroup of H. Again $U = W^n$ now follows.

We now obtain the counterpart of Theorem 2.08:

3.10. Theorem. *The descending chain determined by the fully invariant subgroup V of F is finite, that is it becomes stationary after a finite number of steps, if and only if, V represents the set of all laws of a finitely generated group.*

If k^* is the least integer such that V represents the set of all laws of a group that can be generated by k^* elements, then

$$W^{k^*-1} > W^{k^*} = W^{k^*+1} = \cdots = V.$$

Proof. If $W^n = V$ for some n, then by definition of W^n, V represents the set of all laws of F_n/V_n, which is generated by n elements. Conversely, if V is the set of all laws of a finitely generated group H, generated by n elements (say), then Theorem 3.08 shows that W^n represents the set of all laws holding in every n-generator group of the variety determined by V, that is, the laws of W^n hold in particular in the group H itself. Therefore $W^n \leqq V$, and so $W^n = V$. The remaining statement of the theorem now follows immediately.

Again it is not known whether every variety can be defined, according to 1.05, by a finitely generated group. Nor is it known whether one of the two chains being finite implies that the other chain also must be finite. If this is true at all, then the two chains certainly need not have the same length. This is shown by the example of the BURNSIDE variety of exponent three, which we discuss as illustration. The facts are, of course, not new: they are due to LEVI and VAN DER WAERDEN ([8]; cf. also [14]), whose results we quote.

3.11. Example. We take V as the fully invariant closure in F of the single word $3e_1$. Thus the ascending chain consists of one term only; $V^{(1)} = V$, $k = 1$.

Next we consider the free groups of rank 1, 2, and 3 of the variety; these are respectively the cycle of order three, and the BURNSIDE groups $B_{2,3} \cong F_2/V_2$ and $B_{3,3} \cong F_3/V_3$. Thus W^1 determines the variety of all abelian groups of exponent three. Further, in both, $B_{2,3}$ and $B_{3,3}$, the law $[x, y, y] = 0$ holds; hence $[e_1, e_2, e_2]$ belongs to V_2, and therefore to every V_n and to V. But $B_{2,3}$ also satisfies the law $[x, y, z] = 0$, while $B_{3,3}$ does not; hence $[e_1, e_2, e_3]$ belongs to W^2, but not to W^3. Finally, all the laws of $B_{3,3}$ also hold in every group $B_{n,3} \cong F_n/V_n$ for $n \geq 3$; hence

$$W^1 > W^2 > W^3 = V, \qquad \text{and so } k^* = 3.$$

It is perhaps not superfluous to show, following the method of this paragraph, how the word $[e_1, e_2, e_3]$, which does not belong to V_3 (and therefore not to W^3, by 3.03), comes to belong to W^2. We recall that W^2 is the greatest fully invariant subgroup of F contained in $\{V, F_2^*\} = \{V_2, F_2^*\}$. Writing x^y for $-y + x + y$, we have:

$$[e_1, e_2, e_3] = -e_3^{[e_1, e_2]} + e_3 \in F_2^* \leqq \{V, F_2^*\}.$$

To show that $[e_1, e_2, e_3]$ belongs to W^2, one has to confirm that every substitution of words x, y, z of F for e_1, e_2, e_3 results in an element of $\{V_2, F_2^*\}$. Now $[x, y, z]$ may be expanded into a sum of commutators of the form $[e_i, e_j, e_k]$

and their transforms. But every such commutator—and therefore also its transforms—belongs to $\{V_2, F_2^*\}$: namely to F_2^*, if all i, j, k are greater than 2; and to V_2, if all i, j, k are equal to 1 or 2. For the remaining cases, $[e_1, e_2, e_k]$ and $[e_1, e_j, e_k]$ with $j, k > 2$ are typical. But

$$[e_1, e_2, e_k] = -e_k^{[e_1, e_2]} + e_k, \quad \text{and} \quad [e_1, e_j, e_k] = [-e_j^{e_1} + e_j, e_k];$$

hence both belong to F_2^*, and therefore to $\{V_2, F_2^*\}$.

Part II

4. The near-ring of endomorphisms of a reduced free group

We consider a fixed reduced free group $G_n \cong F_n/V_n$. At present the rank n may be any finite or infinite cardinal, although we shall restrict ourselves later to finite or countably infinite rank. A basis of G_n, that is, a set of free generators $e_1, e_2, \ldots, e_n$ is chosen, and will remain fixed. Its characteristic property is that every mapping of these generators into the group can be continued to an endomorphism of the group. More precisely:

Every element $g \in G_n$ is representable as a word in the generators $e_1, e_2, \ldots$, $g = g(e_1, \ldots, e_n) = g(\mathfrak{e})$, where $\mathfrak{e}$ stands for the ordered set $e_1, e_2, \ldots, e_n$. This representation is not unique; two words represent the same element of G_n if, and only if, interpreted as elements of the absolutely free group F_n on the same generators e_i, they differ by an element of V_n. Now an endomorphism α of G_n is determined by the images $a_i(\mathfrak{e}) \in G_n$ of the basis elements e_i; the a_i may be arbitrarily chosen, the map of any element g of G_n is then determined:

4.01. *If α is given by $e_i\alpha = a_i(\mathfrak{e})$, $a_i(\mathfrak{e}) \in G_n$ for all i, then*

$$g(e_1, e_2, \ldots, e_n)\,\alpha = g(e_1\alpha, e_2\alpha, \ldots, e_n\alpha) = g(a_1, a_2, \ldots, a_n),$$

or briefly: $g(\mathfrak{e})\,\alpha = g(\mathfrak{a})$.

Because V_n is fully invariant in F_n, only the particular word $g(\mathfrak{a})$, not the element it represents in G_n, depends on the words chosen to represent g and the elements a_i. If now we interpret the ordered set of elements a_i as a vector whose n components are the elements a_i of G_n, then:

4.02. *The set of all endomorphisms α of G_n is represented by the set of all vectors with n components a_i in G_n, the representation being given by $e_i\alpha = a_i$ for all i.*

Two vectors represent the same endomorphism if, and only if, corresponding components, interpreted as elements of F_n, are congruent modulo V_n.

Accordingly, we may now always interpret a small Greek letter as signifying either an endomorphism of G_n or an n-vector with components in G_n. This dual interpretation will prove useful.

4.03. Definition. *If α and β are endomorphisms of G_n, then the the sum and the product of α and β are, respectively, the endomorphisms given by:*

$$e_i(\alpha + \beta) = e_i\alpha + e_i\beta \quad \text{and} \quad e_i(\alpha\beta) = (e_i\alpha)\,\beta, \quad \text{for all } i.$$

Note that, because α and β are homomorphisms, the product of two endomorphisms is defined in agreement with the customary definition of the product of two mappings. But not so the sum: The sum of two mappings μ, ν of a group H into itself is usually defined as the mapping given by $h(\mu+\nu)=h\mu+h\nu$ for *all* $h \in H$, and is therefore not in general an endomorphism of H, even if μ and ν both are endomorphisms. In our case, $\alpha+\beta$ is by definition an endomorphism; but 4.01 shows that the map of an arbitrary element g under $\alpha+\beta$ differs in general from $g\alpha+g\beta$, as G_n is not in general abelian.

The algebraic system of all endomorphisms of G_n with addition and multiplication defined by 4.03 will be denoted by Γ_n. Expressing the algebraic operations in Γ_n in terms of the vector representation, we have:

4.04. *If α has components a_i, and β has components b_i, then $\alpha+\beta$ and $\alpha\beta$ are given by*

$$e_i(\alpha+\beta) = a_i(\mathfrak{e}) + b_i(\mathfrak{e}) \qquad \text{for all } i,$$

and

$$e_i(\alpha\beta) = a_i(\mathfrak{b}) = a_i(b_1, \ldots, b_n) \qquad \text{for all } i.$$

Thus, the sum of the endomorphisms is represented by the sum of the vectors; the product is represented by the map of the vector α under the endomorphism β. Or, expressed differently, a product $\alpha\beta$ may be read either as a product of two endomorphism, or as the map of the vector α under the endomorphism β, whichever is more useful in the context. This shows almost immediately:

4.05. Theorem. *Γ_n is a near-ring. More precisely: 1. Γ_n is a semigroup under multiplication, with an identity element ε given by $e_i\varepsilon = e_i$ for all i. 2. Γ_n is a group with respect to addition; the additive group is the cartesian (or unrestricted direct) sum of n isomorphic copies of G_n. The zero of addition, also denoted by 0, is a two-sided zero of multiplication. 3. Γ_n satisfies the right distributive law, $(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$ for all $\alpha, \beta, \gamma \in \Gamma_n$.*

Proof. The first statement follows from the interpretation of $\alpha\beta$ as a product of endomorphisms; the second from the interpretation of $\alpha+\beta$ as a sum of two n-vectors with components in G_n. The distributive law is confirmed directly from 4.03:

$$\begin{aligned} e_i(\alpha+\beta)\gamma = (e_i\alpha + e_i\beta)\gamma &= (e_i\alpha)\gamma + (e_i\beta)\gamma, && \text{as } \gamma \text{ is homomorphic,} \\ &= e_i(\alpha\gamma+\beta\gamma), && \text{for all } i. \end{aligned}$$

The endomorphism 0 maps every element, hence every vector, onto 0; therefore $\alpha 0 = 0$ for all α. But $0\alpha = 0$ follows from the distributive law, so that 0 is, in fact, the two-sided zero of multiplication.

The multiplicative semigroup, and the additive group, of Γ_n will be denoted by $\Gamma_n(\cdot)$ and $\Gamma_n(+)$ respectively. The k^{th} summand of $\Gamma_n(+)$ in its representation as cartesian sum consists of all endomorphisms α^k,

4.06 $$e_i\alpha^k = 0 \quad \text{for} \quad i \neq k, \qquad e_k\alpha_k = a_k(\mathfrak{e}) \quad \text{with} \quad a_k(\mathfrak{e}) \in G_n.$$

If in particular we denote by ε_j^k the endomorphism given by

4.07 $$e_i\varepsilon_j^k = 0 \quad \text{for} \quad i \neq k, \qquad e_k\varepsilon_j^k = e_j,$$

then every element α^k is a finite (non-commutative) sum of elements ε_j^k,

$$\alpha^k = \sum_j n_j \varepsilon_j^k, \qquad \text{where the } n_j \text{ are integers.}$$

Hence we have from the structure of $\Gamma_n(+)$:

4.08. Theorem. *If n is finite, every element of Γ_n is a finite sum of integral multiples of the n^2 elements ε_j^k.*

The significance of the theorem stems from the following fact:

4.09. Theorem. *In every near-ring Γ_n, every element ε_j^k distributes also as left-hand factor,*

$$\varepsilon_j^k(\alpha + \beta) = \varepsilon_j^k \alpha + \varepsilon_j^k \beta \qquad \textit{for all } j, k \textit{ and all} \qquad \alpha, \beta \in \Gamma_n.$$

Proof. As ε_j^k maps the i^{th} generator onto zero, whenever $i \neq k$, and zero is mapped onto itself by every endomorphism, it follows that the i^{th} component of both, the right-hand and the left-hand side, is zero. For the k^{th} components we have

$$e_k \varepsilon_j^k(\alpha + \beta) = e_j(\alpha + \beta) = e_j \alpha + e_j \beta = e_k \varepsilon_j^k \alpha + e_k \varepsilon_j^k \beta = e_k(\varepsilon_j^k \alpha + \varepsilon_j^k \beta).$$

The preceding remarks show that we may think of Γ_n as a generalized matrix ring. The "matrix" representing α is given by:

$$\alpha \leftrightarrow [a_i(e_j)] = \begin{pmatrix} a_1(e_1, e_2, \ldots, e_n) \\ \ldots\ldots\ldots\ldots \\ a_n(e_1, e_2, \ldots, e_n) \end{pmatrix};$$

that is, the "rows" correspond to the components of α, the "columns" to the ordered set of generators e_i. If n is infinite, the "matrices" still are row-finite. The multiplication rule is given by

$$\alpha\beta \leftrightarrow [a_i(e_j)]\,[b_j(e_k)] = [a_i(b_j(e_k))].$$

If G_n is a free abelian group, this interpretation gives precisely the representation of the ring of endomorphisms as a ring of matrices over the integers (or over the integers modulo m, if G_n is the free abelian group of exponent m).

We conclude this paragraph with a discussion of units and right regular elements of $\Gamma_n(\cdot)$. We need a short digression: Deriving from a well known question posed by H. Hopf (cf. e.g. [12]), we call a group H a Hopf-group if it is not isomorphic to a proper factor group of itself. A reduced free group G_n can be a Hopf-group only if n is finite. Whether this condition is sufficient, is an unsolved problem; so far, only certain classes of reduced free groups of finite rank have been shown to be Hopf-groups (cf. e.g. [1], [5], [10]). From the definition we have:

4.10. *A reduced free group G_n of finite rank is a* Hopf-*group if, and only if, every n elements that generate G_n generate it freely.*

With this situation in mind we define:

4.11. Definition. *An element α is a unit of Γ_n, if it possesses a unique (right- and left-)inverse α^{-1} in Γ_n.*

An element α of Γ_n is right regular, if $\zeta\alpha = \eta\alpha$ implies $\zeta = \eta$; or, equivalently, if $\xi\alpha = 0$ implies $\xi = 0$.

Clearly, the units of Γ_n are exactly the automorphisms of G_n. Every unit is right regular, and the right regular elements of Γ_n are exactly the iso-endomorphisms of G_n, that is the isomorphic mappings of G_n into itself.

4.12. Theorem. *The relation $\alpha\beta = \varepsilon$ in Γ_n implies that α, or equivalently β, is a unit (and then $\beta = \alpha^{-1}$) if, and only if, the group G_n is a* HOPF*-group.*

Proof. Assume first that G_n is a HOPF-group, and that $\alpha\beta = \varepsilon$ in Γ_n. If α and β have components a_i and b_i respectively, we have therefore $a_i(b_1, \ldots, b_n) = e_i$ for $i = 1, \ldots, n$. Hence the elements $b_1, \ldots, b_n$ generate G_n, and therefore generate it freely. This means that the mapping β given by $e_i\beta = b_i$ $(i = 1, \ldots, n)$ is an automorphism of G_n, and β^{-1} exists. But then $(\alpha\beta)\beta^{-1} = \beta^{-1} = \alpha(\beta\beta^{-1}) = \alpha$, and so α also is a unit.

Next assume that G_n is not a HOPF-group, that is, it possesses a proper factor group isomorphic to itself. The natural homomorphism onto this factor group followed by the isomorphism of the factor group onto G_n constitutes a proper endomorphism β of G_n. Let $e_i\beta = b_i$ $(i = 1, \ldots, n)$. Since β is a mapping onto G_n, there exist elements a_i in G_n such that $a_i\beta = e_i$ $(i = 1, \ldots, n)$. We define α by $e_i\alpha = a_i$ $(i = 1, \ldots, n)$. Then $e_i\alpha\beta = e_i$ for all i, hence $\alpha\beta = \varepsilon$. But β is a proper endomorphism and so possesses no inverse, which proves 4.12.

We note that the α of the proof is right regular: $\xi\alpha = 0$ implies $(\xi\alpha)\beta = 0 = \xi(\alpha\beta) = \xi$. Thus α is an iso-endomorphism, and our proof gives as corollary:

4.13. BAER'S Theorem ([1]). *If a reduced free group is isomorphic to a proper factor group, then also to a proper subgroup.*

5. The near-ring Γ_ω

We now assume n to be finite or countably infinite, so that the near-rings are those corresponding to reduced free groups of finite or countably infinite rank. The latter will now be denoted again by G, without subscript. However, we restrict ourselves even further: since $\Gamma_{\aleph_0}(+)$ is the unrestricted direct sum of $\aleph_0$ copies of G, Theorem 4.08 does not hold. But the existence of a "distributive basis" as given by 4.08 and 4.09 is essential for the ideal theory, which we wish to use. We therefore consider only a sub-near-ring Γ_ω of $\Gamma_{\aleph_0}$, namely—in terms of the generalized matrix representation—the near-ring of all row- and column-finite matrices of $\Gamma_{\aleph_0}$.

For every finite n we consider the subset of $\Gamma_{\aleph_0}$ consisting of all those endomorphisms α whose first n components involve only the generators $e_1, \ldots, e_n$, and whose remaining components are zero:

$$e_i\alpha = a_i(e_1, \ldots, e_n) \quad \text{for} \quad i = 1, \ldots, n; \qquad e_i\alpha = 0 \quad \text{for} \quad i > n.$$

Evidently these elements form a near-ring contained in $\Gamma_{\aleph_0}$ which is isomorphic to Γ_n. We denote it by the the same symbol Γ_n without danger of

confusion. Then $\Gamma_1 < \Gamma_2 < \cdots < \Gamma_n < \cdots$, and we put

$$\Gamma_\omega = \bigcup_n \Gamma_n. \tag{5.01}$$

Γ_ω is clearly a near-ring; it consists of all those endomorphisms of G which map the subgroup generated by $e_1, \ldots, e_n$ (for some n) into itself, and the complimentary subgroup on zero.

The additive group $\Gamma_\omega(+)$ of Γ_ω is the (restricted) direct sum of countably many isomorphic copies of G. Hence the essential basis property holds; we summarise it for the case of Γ_ω:

5.02. Theorem. *If ε_j^k is given by $e_i \varepsilon_j^k = 0$ for $i \neq k$, and $e_k \varepsilon_j^k = e_j$, then*
(i) *every element $\xi \in \Gamma_\omega$ is a finite sum of integral multiples of elements ε_j^k,*

$$\xi = \sum_{j,k} n_{j,k} \varepsilon_j^k \qquad (n_{j,k} \text{ integers});$$

(ii) *every ε_j^k distributes also as left-hand factor,*

$$\varepsilon_j^k(\alpha + \beta) = \varepsilon_j^k \alpha + \varepsilon_j^k \beta \quad \text{for all } j, k \text{ and all } \alpha, \beta \in \Gamma_\omega.$$

The near-ring Γ_ω possesses no identity element, nor does it possess units or right-regular elements. We call the identity elements of its sub-near-rings Γ_n "relative identities", and denote them by ε_n. The ε_n are just the retractive endomorphisms considered in the case of the absolutely free groups in § 1. As then, they can again be used to pick out mechanically the near-rings Γ_n from the whole of Γ_ω:

5.03. *An element ξ of Γ_ω belongs to Γ_n if, and only if, $\varepsilon_n \xi \varepsilon_n = \xi$. For any element η of Γ_ω, $\varepsilon_n \eta \varepsilon_n$ belongs to Γ_n, and $\Gamma_n = \varepsilon_n \Gamma_\omega \varepsilon_n$.*

Proof. If $\xi \in \Gamma_n < \Gamma_\omega$, then $\varepsilon_n \xi \varepsilon_n = \xi$, as ε_n is the identity of Γ_n. Conversely, if $\xi = \varepsilon_n \xi \varepsilon_n$, then only the first n components of ξ are non-trivial, because the first factor ε_n has this property; and ξ depends on $e_1, \ldots, e_n$ only, because the last factor ε_n has this property.

If $\eta \in \Gamma_\omega$, then $\varepsilon_n \eta \varepsilon_n = \varepsilon_n^2 \eta \varepsilon_n^2$, hence $\varepsilon_n \eta \varepsilon_n \in \Gamma_n$ by the first part. Therefore $\varepsilon_n \Gamma_\omega \varepsilon_n \subseteq \Gamma_n$. But also $\Gamma_n = \varepsilon_n \Gamma_n \varepsilon_n \subseteq \varepsilon_n \Gamma_\omega \varepsilon_n$, hence $\Gamma_n = \varepsilon_n \Gamma_\omega \varepsilon_n$.

Further, one confirms easily:

5.04. *Every ε_n distributes also as left-hand factor: $\varepsilon_n(\alpha + \beta) = \varepsilon_n \alpha + \varepsilon_n \beta$, for all n, and all $\alpha, \beta \in \Gamma_\omega$.*

6. Ideals and homomorphisms of Γ_n and Γ_ω

The relation between ideals and homomorphisms in the near-rings Γ_n and Γ_ω relies entirely on the existence of an additive basis which consists of elements distributing on both sides. Beyond that the fact that these near-rings are in character near-rings of matrices over a group is used essentially. Most statements in this and the following paragraph hold equally in Γ_n and Γ_ω; wherever this is the case we simply use Γ.

6.01. Definition. *The subset $\mathfrak{A}$ of Γ is a left ideal, right ideal, or (two-sided) ideal, if $\mathfrak{A}$ is a normal subgroup of $\Gamma(+)$, and $\xi \mathfrak{A} \subseteq \mathfrak{A}$, $\mathfrak{A} \eta \subseteq \mathfrak{A}$, $\xi \mathfrak{A} \eta \subseteq \mathfrak{A}$ respectively for all $\xi, \eta \in \Gamma$.*

6.02. *For every ideal $\mathfrak{A}$ of Γ, the relation "$\beta \equiv \gamma \bmod \mathfrak{A}$ if, and only if, $\beta - \gamma \in \mathfrak{A}$" is a congruence relation on the near-ring Γ.*

Proof. Since $\mathfrak{A}$ is, by definition, a normal subgroup of $\Gamma(+)$, we need only prove that, if $\beta \equiv \gamma \bmod \mathfrak{A}$ and $\beta' \equiv \gamma' \bmod \mathfrak{A}$, then $\beta\beta' \equiv \gamma\gamma' \bmod \mathfrak{A}$. From the premise we have:

$$\beta = \gamma + \alpha, \quad \beta' = \gamma' + \alpha', \quad \text{where} \quad \alpha, \alpha' \in \mathfrak{A}.$$

Hence

$$\beta\beta' = (\gamma + \alpha)(\gamma' + \alpha') = \gamma(\gamma' + \alpha') + \alpha(\gamma' + \alpha') = \gamma(\gamma' + \alpha') + \alpha'',$$

where $\alpha'' \in \mathfrak{A}$, as $\mathfrak{A}$ is a right ideal. To prove that

$$\gamma(\gamma' + \alpha') = \gamma\gamma' + \alpha^* \qquad \text{with } \alpha^* \in \mathfrak{A},$$

we note that (i) this is true if $\gamma = \varepsilon_j^k$; for then we have

$$\varepsilon_j^k(\gamma' + \alpha') = \varepsilon_j^k\gamma' + \varepsilon_j^k\alpha',$$

where the last term belongs to $\mathfrak{A}$, since $\mathfrak{A}$ is a left ideal;

(ii) if $\gamma_1(\gamma' + \alpha') = \gamma_1\gamma' + \alpha_1$ and $\gamma_2(\gamma' + \alpha') = \gamma_2\gamma' + \alpha_2$ with $\alpha_1, \alpha_2 \in \mathfrak{A}$, then

$$\begin{aligned}(\gamma_1 + \gamma_2)(\gamma' + \alpha') &= \gamma_1(\gamma' + \alpha') + \gamma_2(\gamma' + \alpha') = \gamma_1\gamma' + \alpha_1 + \gamma_2\gamma' + \alpha_2 \\ &= \gamma_1\gamma' + \gamma_2\gamma' - \gamma_2\gamma' + \alpha_1 + \gamma_2\gamma' + \alpha_2 = (\gamma_1 + \gamma_2)\gamma' + \alpha_3,\end{aligned}$$

where α_3 belongs to $\mathfrak{A}$, as $\mathfrak{A}$ is a normal subgroup of $\Gamma(+)$. By 4.08 and 5.02 every element γ is a finite sum of elements ε_j^k; therefore (i) and repeated application of (ii) prove 6.02.

It now follows in the usual way that addition and multiplication of congruence classes can be defined in the natural manner, and that the congruence classes then form a near-ring, the quotient near-ring $\Gamma/\mathfrak{A}$. The mapping which maps every element of Γ on its class modulo $\mathfrak{A}$ is a homomorphism of Γ onto $\Gamma/\mathfrak{A}$, of which $\mathfrak{A}$ is the kernel. Conversely, if $\hat{\varrho}$ is any homomorphic mapping of Γ onto a near-ring $\Gamma\hat{\varrho} = \hat{\Gamma}$, then the kernel of the mapping is an ideal $\mathfrak{A}$ of Γ. For it is clearly a normal subgroup of $\Gamma(+)$; and if $\alpha \in \mathfrak{A}$, that is $\alpha\hat{\varrho} = 0$, then $(\xi\alpha\eta)\hat{\varrho} = \xi\hat{\varrho} \cdot 0 \cdot \eta\hat{\varrho} = 0$, hence $\xi\alpha\eta \in \mathfrak{A}$ for all $\xi, \eta \in \Gamma$. Therefore we have:

6.03. Theorem. *In every near-ring Γ_n or Γ_ω the ideals are precisely the kernels of the homomorphisms of Γ_n or Γ_ω onto a near-ring $\Gamma_n\hat{\varrho}$ or $\Gamma_\omega\hat{\varrho}$ respectively.*

In the usual way one deduces further:

6.04. Theorem. *The map of an ideal (left ideal, right ideal) of Γ under the homomorphism $\hat{\varrho}$ is an ideal (left ideal, right ideal) of $\Gamma\hat{\varrho}$. The ideals (left ideals, right ideals) of $\Gamma\hat{\varrho}$ are in one-one correspondence to those ideals (left ideals, right ideals) of Γ which contain the kernel $\mathfrak{A}$ of $\hat{\varrho}$.*

We turn to an alternative characterization of the ideals (left ideals, right ideals) in terms of the components of their elements. We recall, that the free group associated with Γ is G_n, if $\Gamma = \Gamma_n$, and G_ω if $\Gamma = \Gamma_\omega$.

6.05. Theorem. *The subset $\mathfrak{A}$ of Γ is a left ideal if, and only if, the components of the elements of $\mathfrak{A}$ vary independently over the elements of a normal subgroup N of the free group associated with Γ.*

The subset $\mathfrak{A}$ of Γ is a right ideal if, and only if, it is a normal subgroup of $\Gamma(+)$, and for each fixed i, the i^{th} components of the elements of $\mathfrak{A}$ form a fully invariant subgroup $A(i)$ of the free group associated with Γ.

Corollary. *The subset $\mathfrak{A}$ of Γ is a right ideal if the components of the elements of $\mathfrak{A}$ vary independently over a set of fully invariant subgroups $A(i)$ of the free group associated with Γ.*

Proof. The argument is almost the same in the two cases $\Gamma = \Gamma_n$ and $\Gamma = \Gamma_\omega$. 1. If $\mathfrak{A}$ is a left ideal, it is a normal subgroup of $\Gamma(+)$, hence the set of all i^{th} components of elements of $\mathfrak{A}$ is a normal subgroup $N(i)$ of G_n or G respectively. If $a_i \in N(i)$, there exists an element $\alpha \in G$ such that $e_i \alpha = a_i$. Since $\mathfrak{A}$ is a left ideal, also $\varepsilon_i^k \alpha \in \mathfrak{A}$. But $e_k \varepsilon_i^k \alpha = e_i \alpha = a_i$, hence $a_i \in N(k)$. It follows that for all i and k, $N(i) = N(k) = N$. Now let $a_1, \ldots, a_n$[6]) be any given elements of N. Then a_i occurs as first component of some element α_i of $\mathfrak{A}$. With α_i also $\varepsilon_1^i \alpha_i$ belongs to $\mathfrak{A}$, and

$$e_i \varepsilon_1^i \alpha_i = e_1 \alpha_i = a_i, \qquad e_j \varepsilon_1^i \alpha_i = 0 \quad \text{for } j \neq i. \tag{6.06}$$

But then the sum $\sum_{i=1}^{n} \varepsilon_1^i \alpha_i$ also belongs to $\mathfrak{A}$, and its components are the prescribed elements a_i of N for $i = 1, \ldots, n$, and the remaining components (in the case $\Gamma = \Gamma_\omega$) are zero.

Conversely, if $\mathfrak{A}$ satisfies the premise of the first part of 6.05, it is evidently a normal subgroup of $\Gamma(+)$. Moreover, if $\alpha \in \mathfrak{A}$, and α has components a_i, and if $\xi \in \Gamma$ is any element with components $x_i(e_1, \ldots, e_n)$[6]), then the components of $\xi \alpha$ are the words $x_i(a_1, \ldots, a_n)$[6]) formed with the elements a_i of N, hence they belong to N, and so $\xi \alpha \in \mathfrak{A}$ follows; that is $\mathfrak{A}$ is a left ideal.

2. If $\mathfrak{A}$ is a right ideal of Γ, it is a normal subgroup of $\Gamma(+)$; hence the elements occuring as i^{th} components of elements of $\mathfrak{A}$ form a normal subgroup $A(i)$ of G_n or G respectively. Moreover, if $\alpha \in \mathfrak{A}$, and its i^{th} component is $a_i(e_1, \ldots, e_n)$[6]), let η be any element of Γ with components $y_1, \ldots, y_n$[6]) (and remaining components zero in the case $\Gamma = \Gamma_\omega$). Then the i^{th} component of $\alpha \eta$ is $a_i(y_1, \ldots, y_n)$. But $\alpha \eta \in \mathfrak{A}$, therefore $a_i(y_1, \ldots, y_n) \in A(i)$, which shows that $A(i)$ is a fully invariant subgroup of G_n or G respectively.

Conversely, if the $A(i)$ are fully invariant in the free group associated with Γ, then one confirms in the same way that $\alpha\eta \in \mathfrak{A}$ for all $\eta \in \Gamma$, provided $\alpha \in \mathfrak{A}$. Since $\mathfrak{A}$ is given to be a normal subgroup of $\Gamma(+)$, it follows that it is a right ideal.

If the components of $\mathfrak{A}$ run independently over the fully invariant, that is certainly normal, subgroups $A(i)$, then $\mathfrak{A}$ is ensured to be normal in $\Gamma(+)$; hence the corollary.

[6]) In the case $\Gamma = \Gamma_n$, the n occurring here is the rank n of G_n in the case $\Gamma = \Gamma_\omega$, n is an arbitrary positive integer.

Combining the two parts of 6.05, we finally have for ideals:

6.07. Theorem. *The ideals $\mathfrak{A}$ of Γ are in one-one correspondence with the fully invariant subgroups A of the free group associated with Γ. The correspondence is given by: $\alpha \in \mathfrak{A}$ if, and only if, $e_i \alpha \in A$ for all i.*

Before we use this correspondence between ideals and fully invariant subgroups to give a description of the homomorphic maps of a near-ring Γ, we note a consequence of the proof of 6.05, which we shall use later. In the case of two-sided ideals, it is sufficient to know that $\mathfrak{A}$ is a subgroup of $\Gamma(+)$ which is closed under left- and right multiplication by elements of Γ; it then follows that $\mathfrak{A}$ is a normal subgroup of $\Gamma(+)$:

6.08. *The subset $\mathfrak{A}$ of Γ is an ideal if (and only if) it is closed under addition, and left- and right multiplication by elements of Γ.*

Proof. From the assumptions it follows that $\mathfrak{A}$ is closed under subtraction, hence is a subgroup of $\Gamma(+)$. We have to show that it is a normal subgroup that is, that $\alpha \in \mathfrak{A}$ and $\eta \in \Gamma$ implies $-\eta + \alpha + \eta \in \mathfrak{A}$.

Let α have components $a_1, \ldots, a_n$, η components $y_1, \ldots, y_n$[6]). The left ideal property implies that any component a_i can be "isolated" in $\mathfrak{A}$ (as in 6.06); that is, there belongs to $\mathfrak{A}$ also the element $\varepsilon_i^i \alpha$, for every i, whose only non-zero component is the i^{th} component a_i of α. If $a_i = a_i(e_1, \ldots, e_n)$[6]), and η_i is the element with components $-y_i + e_j + y_i$ $(j = 1, \ldots, n)$, where y_i belongs to G_n or G respectively (and in the case of $\Gamma = \Gamma_\omega$ all further components of η are zero), then the i^{th} component of $\varepsilon_i^i \alpha \eta_i$ is $-y_i + a_i + y_i$, and all its other components are zero. Therefore $-\eta + \alpha + \eta = \sum_{i=1}^{n} \varepsilon_i^i \alpha \eta_i$, which clearly belongs to $\mathfrak{A}$.

The homomorphism of Γ whose kernel is $\mathfrak{A}$ reduces every element of Γ modulo $\mathfrak{A}$, that is it reduces the components of the elements of Γ modulo A. But the factor group of a reduced free group with respect to one of its fully invariant subgroups is itself a reduced free group of the same rank. Therefore the Theorems 6.03 and 6.07 now lead to:

6.09. Theorem. *Every homomorphic map of the near-ring Γ_n or Γ_ω of endomorphisms of the reduced free group G_n or G respectively is itself a near-ring $\bar{\Gamma}_n$ or $\bar{\Gamma}_\omega$. If $\mathfrak{A}$ is the kernel of the homomorphism, A the corresponding fully invariant subgroup of G_n or G respectively, then the reduced free group associated with $\bar{\Gamma}_n$ or $\bar{\Gamma}_\omega$ is the factor group G_n/A or G/A respectively.*

Corollary. *Every near-ring Γ_n or Γ_ω is a homomorphic map of the corresponding near-ring Φ_n or Φ_ω associated with the absolutely free group F_n or F respectively.*

The corollary permits an amusing formulation of HOPF's problem for reduced free groups of finite rank: We have seen (Theorem 4.12) that G_n is a HOPF group if, and only if, $\alpha\beta = \varepsilon$ in Γ_n implies $\beta = \alpha^{-1}$, or equivalently, $\beta\alpha = \varepsilon$. As $\Gamma_n \cong \Phi_n/\mathfrak{A}$, where $\mathfrak{A}$ is the ideal corresponding to the fully invariant subgroup of F_n which defines G_n, we have:

6.10. *Every reduced free group of finite rank is a* HOPF *group (that is, a group not isomorphic to any proper factor group of itself) if, and only if, for every n, and for any two elements α and β of Φ_n, the least ideal containing $\alpha\beta - \varepsilon$ also contains $\beta\alpha - \varepsilon$.*

7. Lattice operations and multiplication of ideals in Γ_n and Γ_ω

Except for the last theorem, this paragraph makes no explicit reference to the underlying free groups; the elementary algebra of ideals depends entirely on the matrix character of the near-rings Γ_n and Γ_ω. Again we write Γ whenever a statement applies equally to Γ_n and Γ_ω.

Immediately from the definition of ideals (6.01) we have:

7.01. *The intersection of two ideals (left ideals, right ideals) of Γ is an ideal (left ideal, right ideal) of Γ.*

7.02. Definition. *The sum $\mathfrak{A}+\mathfrak{B}$ of two ideals (left ideals, right ideals) of Γ is the least ideal (left ideal, right ideal) of Γ containing $\mathfrak{A}$ and $\mathfrak{B}$.*

7.03. *The sum $\mathfrak{A}+\mathfrak{B}$ of two ideals (left ideals, right ideals) consists of all elements of the form $\alpha+\beta$, $\alpha\in\mathfrak{A}$, $\beta\in\mathfrak{B}$.*

Proof. In all three cases, $\mathfrak{A}$ and $\mathfrak{B}$ are normal subgroups of $\Gamma(+)$. Hence the set of all sums $\alpha+\beta$ with $\alpha\in\mathfrak{A}$, $\beta\in\mathfrak{B}$, is the least normal subgroup of $\Gamma(+)$ containing both $\mathfrak{A}$ and $\mathfrak{B}$. That this normal subgroup is closed under right multiplication by elements of Γ, if $\mathfrak{A}$ and $\mathfrak{B}$ are right ideals, follows from the distributive law in Γ. That it is closed under left multiplication by elements of Γ, if $\mathfrak{A}$ and $\mathfrak{B}$ are left ideals, follows from the existence of a distributive basis for Γ. One has

(i) $$\varepsilon_i^k(\alpha+\beta)=\varepsilon_j^k\alpha+\varepsilon_j^k\beta=\alpha'+\beta';$$

and

(ii) if $\xi_1(\alpha+\beta)=\alpha_1+\beta_1$ and $\xi_2(\alpha+\beta)=\alpha_2+\beta_2$,

then

$$\begin{aligned}(\xi_1+\xi_2)(\alpha+\beta)&=\xi_1(\alpha+\beta)+\xi_2(\alpha+\beta)=\alpha_1+\beta_1+\alpha_2+\beta_2\\&=\alpha_1+\alpha_2-\alpha_2+\beta_1+\alpha_2+\beta_2=\alpha_3+\beta_3,\end{aligned}$$

because $-\alpha_2+\beta_1+\alpha_2$ belongs to $\mathfrak{B}$, as $\mathfrak{B}$ is normal in $\Gamma(+)$.

(i) and repeated application of (ii) give $\xi(\alpha+\beta)=\alpha''+\beta''$ for all $\xi\in\Gamma$. It is clear from Theorem 6.07 that:

7.04. *The fully invariant subgroups corresponding to the intersection and to the sum of two ideals $\mathfrak{A}$ and $\mathfrak{B}$ are the intersection and the sum respectively of the fully invariant subgroups corresponding to $\mathfrak{A}$ and $\mathfrak{B}$.*

The two-step argument used in 7.03 shows further:

7.05. *The ideal generated by a set of elements α_i of Γ, that is, the least ideal containing the elements α_i, consists of all finite sums of the form $\sum_i \xi_i\alpha_i\eta_i$, $\xi_i,\eta_i\in\Gamma$ (where, of course, the same element α_i may occur repeatedly with different left- and right factors).*

Proof. Every sum $\sum_i \xi_i \alpha_i \eta_i$ clearly belongs to every ideal containing the elements α_i. It therefore remains to show that the set of all such sums is itself an ideal. We use 6.08: The set of all these sums is additively closed; it is closed under right multiplication because of the distributive law; finally $\xi \sum \xi_i \alpha_i \eta_i = \sum \xi_i' \alpha_i \eta_i'$ for every $\xi \in \Gamma$, because (i) this is true when $\xi = \varepsilon_j^k$, as this distributes over the sum; and (ii) if $\xi_1 \sum \xi_i \alpha_i \eta_i = \sum \xi_i' \alpha_i \eta_i'$ and $\xi_2 \sum \xi_i \alpha_i \eta_i = \sum \xi_i'' \alpha_i \eta_i''$, then, using the distributive law,

$$(\xi_1 + \xi_2) \sum \xi_i \alpha_i \eta_i = \sum \xi_i' \alpha_i \eta_i' + \sum \xi_i'' \alpha_i \eta_i'',$$

and this is itself a finite sum of the same form.

Now we define the product of ideals in the usual way:

7.06. Definition. *The product $\mathfrak{A}_l \mathfrak{B}_r$ of a left ideal $\mathfrak{A}_l$ and a right ideal $\mathfrak{B}_r$ of Γ is the ideal generated in Γ by all products $\alpha\beta$, where $\alpha \in \mathfrak{A}_l$ and $\beta \in \mathfrak{B}_r$.*

As $\xi \alpha \beta \eta = (\xi \alpha)(\beta \eta) = \alpha' \beta'$, $\alpha' \in \mathfrak{A}_l$, $\beta' \in \mathfrak{B}_r$, 7.05 gives:

7.07. Theorem. *The product $\mathfrak{A}_l \mathfrak{B}_r$ consists of all finite sums of the form $\sum \alpha_i \beta_i$, where $\alpha_i \in \mathfrak{A}_l$, $\beta_i \in \mathfrak{B}_r$.*

If both factors are two-sided ideals $\mathfrak{A}$, $\mathfrak{B}$, then each term $\alpha_i \beta_i$ belongs to $\mathfrak{A} \cap \mathfrak{B}$, and this is additively closed. Hence:

7.08. *If $\mathfrak{A}$ and $\mathfrak{B}$ are ideals of Γ, then $\mathfrak{A}\mathfrak{B} \subseteq \mathfrak{A} \cap \mathfrak{B}$.*

By way of illustration we mention here the *mutual commutator ideal* $[\mathfrak{A}, \mathfrak{B}]$ of two ideals $\mathfrak{A}$ and $\mathfrak{B}$. It is the ideal corresponding to the mutual commutator group $[A, B]$ of A and B, itself a fully invariant subgroup of the group associated with Γ. The ideal $[\mathfrak{A}, \mathfrak{B}]$ is the product of the ideal corresponding to the derived group, briefly the derived ideal, as left hand factor with the right ideal consisting of all those elements of Γ, whose first components lie in A, whose second components lie in B, and whose further components are zero (cf. the corollary of 6.05). One has:

7.09. $[\mathfrak{A}, \mathfrak{B}] \subseteq \mathfrak{A} \cap \mathfrak{B}$ *for any two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of Γ.*

We put together some of the relations between the lattice operations and ideal multiplication which hold in every near-ring Γ. As usual, the ideal consisting of the zero endomorphism only acts as a zero of multiplication, the whole near-ring Γ acts as the two-sided identity of ideal multiplication. Further:

7.10. $\mathfrak{A}(\mathfrak{B}_1 \cap \mathfrak{B}_2) \subseteq \mathfrak{A}\mathfrak{B}_1 \cap \mathfrak{A}\mathfrak{B}_2$, $(\mathfrak{B}_1 \cap \mathfrak{B}_2)\mathfrak{A} \subseteq \mathfrak{B}_1\mathfrak{A} \cap \mathfrak{B}_2\mathfrak{A}$.
This is an immediate consequence of 7.07.

7.11. $(\mathfrak{B}_1 + \mathfrak{B}_2)\mathfrak{A} = \mathfrak{B}_1\mathfrak{A} + \mathfrak{B}_2\mathfrak{A}$; $\quad \mathfrak{A}\mathfrak{B}_1 + \mathfrak{A}\mathfrak{B}_2 \subseteq \mathfrak{A}(\mathfrak{B}_1 + \mathfrak{B}_2)$,
$\mathfrak{A}(\mathfrak{B}_1 + \mathfrak{B}_2) \subseteq \mathfrak{A}\mathfrak{B}_1 + \mathfrak{A}\mathfrak{B}_2 + \mathfrak{A} \cap [\mathfrak{B}_1, \mathfrak{B}_2] \subseteq \mathfrak{A}\mathfrak{B}_1 + \mathfrak{A}\mathfrak{B}_2 + \mathfrak{A} \cap \mathfrak{B}_1 \cap \mathfrak{B}_2$.

The first line follows from 7.03 and 7.07; the second from the fact that $\alpha(\beta_1 + \beta_2)$ differs from $\alpha\beta_1 + \alpha\beta_2$ by elements in the mutual commutator $[\mathfrak{B}_1, \mathfrak{B}_2]$ which must also belong to $\mathfrak{A}$, as $\mathfrak{A}(\mathfrak{B}_1 + \mathfrak{B}_2) \subseteq \mathfrak{A}$.

We note as a corollary:

7.12. *If* $\mathfrak{A}+\mathfrak{B}=\Gamma$, *then* $\mathfrak{A}\cap\mathfrak{B}=\mathfrak{A}\mathfrak{B}+\mathfrak{B}\mathfrak{A}$.

For then $\mathfrak{A}\cap\mathfrak{B}=(\mathfrak{A}+\mathfrak{B})(\mathfrak{A}\cap\mathfrak{B})=\mathfrak{A}(\mathfrak{A}\cap\mathfrak{B})+\mathfrak{B}(\mathfrak{A}\cap\mathfrak{B})\subseteq\mathfrak{A}\mathfrak{B}+\mathfrak{B}\mathfrak{A}\subseteq\mathfrak{A}\cap\mathfrak{B}$.

7.13. $[\mathfrak{A}_1,\mathfrak{A}_2]\,\mathfrak{B}\subseteq[\mathfrak{A}_1\mathfrak{B},\mathfrak{A}_2\mathfrak{B}]$.

As regards associativity of ideal multiplication, we can only say:

7.14. $(\mathfrak{A}\mathfrak{B})\mathfrak{C}\subseteq\mathfrak{A}(\mathfrak{B}\mathfrak{C})$ *for any three ideals of* Γ.

Proof. The product $(\mathfrak{A}\mathfrak{B})\mathfrak{C}$ consists, by 7.07, of all finite sums whose terms are of the form $(\sum\alpha_i\beta_i)\gamma=\sum\alpha_i\beta_i\gamma$; hence it consists of all sums of the form $\sum\alpha\beta\gamma$. The product $\mathfrak{A}(\mathfrak{B}\mathfrak{C})$ consists of all sums of the form $\sum_i\alpha_i\{\sum_j\beta_{i,j}\gamma_{i,j}\}$. Clearly the sums $\sum\alpha\beta\gamma$ which are the elements of $(\mathfrak{A}\mathfrak{B})\mathfrak{C}$, occur amongst these.

We shall see (9.12) that in a near-ring Γ_n of finite rank the inclusion may be proper. Thus ideal multiplication need not be associative, in fact not even power associative. The restriction to a finite number of generators will prove the reason for the non-associativity; this is born out by the fact that in Γ_ω ideal multiplication is associative:

7.15. Theorem. *For any three ideals* $\mathfrak{A}$, $\mathfrak{B}$, *and* $\mathfrak{C}$ *of* Γ_ω

$$(\mathfrak{A}\mathfrak{B})\mathfrak{C}=\mathfrak{A}(\mathfrak{B}\mathfrak{C}).$$

This follows at once from

7.16. Theorem. *The product* $\mathfrak{A}\mathfrak{B}$ *of two ideals of* Γ_ω *consists of all products* $\alpha\beta$, $\alpha\in\mathfrak{A}$, $\beta\in\mathfrak{B}$.

Again, by means of 7.07, this follows by repeated application of:

7.17. *If* $\mathfrak{A}$, $\mathfrak{B}$ *are ideals of* Γ_ω, *and* α_1, α_2 *are elements of* $\mathfrak{A}$, β_1, β_2 *are elements of* $\mathfrak{B}$, *then there exist elements* $\alpha\in\mathfrak{A}$, $\beta\in\mathfrak{B}$, *such that* $\alpha_1\beta_1+\alpha_2\beta_2=\alpha\beta$.

Proof. We introduce for every integer n some special endomorphisms of Γ_ω. Let σ_n be the endomorphism given by

$$\begin{aligned} e_i\sigma_n &= e_{i+n} \quad \text{for} \quad i=1,\dots,n,\\ e_i\sigma_n &= 0 \quad \text{for} \quad i>n. \end{aligned}$$

Let τ_n be the endomorphism given by

$$\begin{aligned} e_i\tau_n &= 0 \quad \text{for} \quad i=1,\dots,n,\\ e_i\tau_n &= e_{i-n} \quad \text{for} \quad i=n+1,\dots,2n,\\ e_i\tau_n &= 0 \quad \text{for} \quad i>2n. \end{aligned}$$

Right multiplication by σ_n replaces the generators $e_1,\dots,e_n$ in an element $\alpha\in\Gamma_n\subset\Gamma_\omega$ by $e_{n+1},\dots,e_{2n}$. Left multiplication by τ_n of an element $\alpha\in\Gamma_n\subset\Gamma_\omega$ has the effect of moving the first n components of α "down" to form the $(n+1)^{\text{st}},\dots,(2n)^{\text{th}}$ components, and replacing the first n components by zeros.

Now let n be the least integer such that the given elements α_1, α_2 and β_1, β_2 all lie in the sub-near-ring Γ_n of Γ_ω. Then

$$7.18. \qquad \alpha_1\beta_1 + \alpha_2\beta_2 = (\alpha_1 + \alpha_2\sigma_n)(\beta_1 + \tau_n\beta_2),$$

where $$\alpha_1 + \alpha_2\sigma_n = \alpha \in \mathfrak{A}, \quad \text{and} \quad \beta_1 + \tau_n\beta_2 = \beta \in \mathfrak{B}.$$

This is easily checked by means of the rules 4.04 for calculating the components of the sum and product of endomorphisms, observing that the four elements $\alpha_1, \alpha_2, \beta_1, \beta_2$ all have only n non-trivial components, which depend on $e_1, \ldots, e_n$ only.

The proof clearly depends on the possibility to use an unlimited number of generators.

A number of questions naturally arise out of these last theorems which seem to make ideal multiplication in Γ_ω quite tractable; there are in particular the problems arising out of the notion of ideal bases. One might hope that at least in Γ_ω the product of two finitely based ideals is itself finitely based. However, what little information is available, consists of isolated examples treated by ad hoc methods. A brief summary of these is given in the Appendix.

It remains to interpret ideal multiplication in the free group associated with Γ.

Notation. The fully invariant subgroup corresponding to the product $\mathfrak{A}\mathfrak{B}$ of two ideals of Γ is denoted by $A \circ B$.

The rule 4.04 for forming the product of two elements of the near-ring shows that $A \circ B$ is the fully invariant subgroup obtained by substituting the elements of B for the generators in the words representing the elements of A and taking the additive closure. Moreover:

7.19. Theorem. *The fully invariant subgroup $A \circ B$ of the free group associated with Γ corresponding to the ideal product $\mathfrak{A}\mathfrak{B}$ in Γ is a fully invariant subgroup of B.*

Proof. As $\mathfrak{A}\mathfrak{B} \subseteq \mathfrak{B}$, certainly $A \circ B \subseteq B$; now $A \circ B$ is generated by all elements of the form $a(b_1, \ldots, b_n)$ [6]), where $a(e_1, \ldots, e_n) \in A$, and $b_1, \ldots, b_n \in B$. But the set of all such elements is closed under endomorphisms of B; for any such endomorphism maps the set $b_1, \ldots, b_n$ onto some set of elements $b_1', \ldots, b_n' \in B$, and as it is a homomorphic mapping, it maps the word $a(b_1, \ldots, b_n)$ onto the word $a(b_1', \ldots, b_n')$, that is on an element of the generating set of $A \circ B$.

The converse of this last theorem is not true in general, as will be seen in the last paragraph; again the restriction to a finite number of generators in the near-rings Γ_n is the reason.

8. The lattice of ideals and ideal multiplication in Φ_ω

From now on we consider the near-rings associated with the absolutely free groups F_n and F only. All we really need is that the free groups we use

have the SCHREIER property that every subgroup is itself a free group. However, this further restriction is not likely to make much difference: we are not concerned with the case of abelian varieties, that is, the theory of ordinary matrix rings. But no non-abelian free groups with the SCHREIER property other than the absolutely free groups are known at present. On the other hand, much of the general picture given in the next two paragraphs remains true also for the near-rings associated with arbitrary varieties; the differences are caused, roughly speaking, by the homomorphism of the near-rings Φ onto the near-rings Γ obliterating distinctions that exist in the near-rings associated with the absolutely free groups.

The semigroup of ideals in Φ_ω is our first concern; the results will be used in the next paragraph to clarify the reason for the non-associativity of ideal multiplication in Φ_n by "reduction to Φ_n" in the sense of § 2.

We show first that in Φ_ω Theorem 7.19 possesses a converse:

8.01. *If B and C are fully invariant subgroups of F, and C is a fully invariant subgroup of B, if further $\mathfrak{B}$ and $\mathfrak{C}$ are the ideals of Φ_ω corresponding to B and C, then there exists an ideal $\mathfrak{A}$ such that $\mathfrak{C}=\mathfrak{A}\mathfrak{B}$.*

Proof. Since C is fully invariant in B, it is a word subgroup of the free group B. This means: if $b_1, b_2, \ldots$ form a set of free generators of B, there exists a set of words $a_i(b_j)$ in these free generators such that C is the fully invariant closure in B of this set of words. Consider the corresponding words $a_i(e_j)$ of F; let A be their fully invariant closure in F, and $\mathfrak{A}$ the ideal of Φ_ω corresponding to A. Then one confirms easily that $\mathfrak{C}=\mathfrak{A}\mathfrak{B}$. One sees why this need not be true in Φ_n: the words defining C as word subgroup of B may involve more than n generators.

The proof suggets that $\mathfrak{A}$ is uniquely determined by $\mathfrak{B}$ and $\mathfrak{C}$. To confirm this, we return to the free generators $b_1, b_2, \ldots$ of the fully invariant subgroup B. The set b_i is necessarily infinite if $\mathfrak{B}\neq\{0\}$; we denote by β_m the element of Φ_ω given by $e_i\beta_m=b_i$ for $i=1,\ldots,m$, $e_i\beta_m=0$ for $i>m$. If β is any element of $\mathfrak{B}$, its finitely many non-trivial components are representable as words in finitely many b_i, and this representation is unique. Hence:

8.02. *Every $\beta\in\mathfrak{B}$ is representable in the form $\beta=\xi\beta_m$ for some m and an element $\xi\in\Phi_\omega$ whose components belong to F_m.*

Moreover, since the b_i are free generators of B:

8.03. *If ξ and η are elements of Φ_ω whose components belong to F_m and F_n respectively, then*

$$\xi\beta_m=\eta\beta_n \text{ implies } \xi=\eta.$$

Now we obtain as a first step:

8.04. *If $\mathfrak{A}_1\geqq\mathfrak{A}_2$, and $\mathfrak{A}_1\mathfrak{B}=\mathfrak{A}_2\mathfrak{B}$, where $\mathfrak{B}\neq\{0\}$, then $\mathfrak{A}_1=\mathfrak{A}_2$.*

Proof. Let α_1 be an arbitrary element of $\mathfrak{A}_1$. There exists an m such that the components of α_1 all belong to F_m. We form the product $\alpha_1\beta_m$. It belongs to $\mathfrak{A}_1\mathfrak{B}=\mathfrak{A}_2\mathfrak{B}$; but as element of the latter, it is of the form (by 7.16):

$$\alpha_1\beta_m=\alpha_2\beta \quad \text{with} \quad \alpha_2\in\mathfrak{A}_2,\ \beta\in\mathfrak{B}.$$

Now we use 8.02 to write β in the form $\beta = \eta\beta_n$ with an element η whose components lie in F_n. But then also $\alpha_2\eta$ has components in F_n, and

$$\alpha_1\beta_m = \alpha_2\beta = \alpha_2\eta\beta_n,$$

hence by 8.03, $\alpha_1 = \alpha_2\eta \in \mathfrak{A}_2$, and so $\mathfrak{A}_1 \subseteq \mathfrak{A}_2$, giving $\mathfrak{A}_1 = \mathfrak{A}_2$.

To complete the argument, we introduce the right quotient of any two ideals $\mathfrak{B}$ and $\mathfrak{C}$.

8.05. Definition[7]). *The right quotient* $\mathfrak{C}r\mathfrak{B}$ (*read:* $\mathfrak{C}$ *divided on the right by* $\mathfrak{B}$) *of any two ideals* $\mathfrak{C}$ *and* $\mathfrak{B}$ *is the set of all elements* $\varrho \in \Phi_\omega$ *such that* $\varrho\beta \in \mathfrak{C}$ *for all* $\beta \in \mathfrak{B}$.

A straightforward calculation shows:

8.06. $\mathfrak{C}r\mathfrak{B}$ *is an ideal containing* $\mathfrak{C}$.

If $\mathfrak{B}_1 \subseteq \mathfrak{B}_2$, *then* $\mathfrak{C}r\mathfrak{B}_1 \supseteq \mathfrak{C}r\mathfrak{B}_2$; $\quad \mathfrak{C}r\Phi_\omega = \mathfrak{C}$.

If $\mathfrak{C}_1 \subseteq \mathfrak{C}_2$, *then* $\mathfrak{C}_1 r\mathfrak{B} \subseteq \mathfrak{C}_2 r\mathfrak{B}$.

8.07. Theorem. *If* $\mathfrak{R} = \mathfrak{C}r\mathfrak{B}$, *then* $\mathfrak{R}\mathfrak{B} \subseteq \mathfrak{B} \cap \mathfrak{C}$, *and* $R \circ B$ *is the greatest fully invariant subgroup of* B *contained in* $B \cap C$.

Proof. $\mathfrak{R}$ is an ideal by 8.06, and $\mathfrak{R}\mathfrak{B} \subseteq \mathfrak{B}$ since a product is contained in each factor. Also $\mathfrak{R}\mathfrak{B} \subseteq \mathfrak{C}$ by definition of $\mathfrak{R}$, hence $\mathfrak{R}\mathfrak{B} \subseteq \mathfrak{B} \cap \mathfrak{C}$. By 7.19, $R \circ B$ is fully invariant in B. Let D be any fully invariant subgroup of B contained in $B \cap C$, and let $\mathfrak{D}$ be the corresponding ideal. By 8.01 there exists an ideal $\mathfrak{A}$ such that $\mathfrak{D} = \mathfrak{A}\mathfrak{B}$. Since $\mathfrak{D} \subseteq \mathfrak{C}$, $\mathfrak{A} \subseteq \mathfrak{R}$ by definition of the right quotient. Hence $\mathfrak{D} = \mathfrak{A}\mathfrak{B} \subseteq \mathfrak{R}\mathfrak{B}$, and so $D = A \circ B \subseteq R \circ B$, that is, $R \circ B$ is maximal.

If now, in particular, C is a fully invariant subgroup of B, then $(\mathfrak{C}r\mathfrak{B})\mathfrak{B} = \mathfrak{C}$; and if also $\mathfrak{A}\mathfrak{B} = \mathfrak{C}$, then $\mathfrak{A} \subseteq \mathfrak{C}r\mathfrak{B}$, hence by 8.04: $\mathfrak{A} = \mathfrak{C}r\mathfrak{B}$. Thus we have proved:

8.08. Theorem. *In* Φ_ω, $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ *with* $\mathfrak{B} \neq \{0\}$ *if, and only if,* C *is a fully invariant subgroup of* B. *Here* $\mathfrak{A}$ *is uniquely determined by* $\mathfrak{B}$ *and* $\mathfrak{C}$, *namely* $\mathfrak{A} = \mathfrak{C}r\mathfrak{B}$.

We obtain as corollary:

8.09. Theorem. *In* Φ_ω, $\mathfrak{A}_1\mathfrak{B} = \mathfrak{A}_2\mathfrak{B}$, *where* $\mathfrak{B} \neq \{0\}$, *implies* $\mathfrak{A}_1 = \mathfrak{A}_2$.

The fact that the ideals in Φ_ω form a semigroup with right cancellation suggests carrying the investigation of right multiplication by a fixed ideal a little further. We know already (7.11) that

$$(\mathfrak{A}_1 + \mathfrak{A}_2)\mathfrak{B} = \mathfrak{A}_1\mathfrak{B} + \mathfrak{A}_2\mathfrak{B}.$$

We now prove:

8.10. *In* Φ_ω, $\qquad (\mathfrak{A}_1 \cap \mathfrak{A}_2)\mathfrak{B} = \mathfrak{A}_1\mathfrak{B} \cap \mathfrak{A}_2\mathfrak{B}$.

[7]) The definition should reasonably be extended to any left ideal $\mathfrak{C}$ and its right quotient by the ideal $\mathfrak{B}$; but we make no use of this. The subsequent statements 8.06 and 8.07 remain true, except that in this more general case $\mathfrak{C}r\mathfrak{B}$ need not contain $\mathfrak{C}$. A specific example: $\mathfrak{C}r\Phi_\omega$ corresponds to the greatest fully invariant subgroup of F contained in the normal subgroup corresponding to the left ideal $\mathfrak{C}$ by 6.05.

Proof. Since the right-hand side contains the left-hand side (7.10), we need only prove $\mathfrak{A}_1\mathfrak{V} \cap \mathfrak{A}_2\mathfrak{V} \leqq (\mathfrak{A}_1 \cap \mathfrak{A}_2)\mathfrak{V}$. Let γ be any element of $\mathfrak{A}_1\mathfrak{V} \cap \mathfrak{A}_2\mathfrak{V}$. By 7.16, γ possesses representations

$$\gamma = \alpha_1\beta' = \alpha_2\beta'', \quad \text{where} \quad \alpha_1 \in \mathfrak{A}_1,\ \alpha_2 \in \mathfrak{A}_2,\ \beta', \beta'' \in \mathfrak{V}.$$

We write the elements β' and β'' of $\mathfrak{V}$ in terms of free generators of B as in 8.02: $\beta' = \xi\beta_m$, $\beta'' = \eta\beta_n$, where ξ and η have components in F_m and F_n respectively. Then $\gamma = \alpha_1\xi\beta_m = \alpha_2\eta\beta_n$, where $\alpha_1\xi$ and $\alpha_2\eta$ also have components in F_m and F_n respectively. Hence, by 8.03, $\alpha_1\xi = \alpha_2\eta$. But $\alpha_1\xi \in \mathfrak{A}_1$, $\alpha_2\eta \in \mathfrak{A}_2$, hence $\alpha_1\xi = \alpha_2\eta = \alpha \in \mathfrak{A}_1 \cap \mathfrak{A}_2$, and so we have $\gamma = \alpha\beta_m \in (\mathfrak{A}_1 \cap \mathfrak{A}_2)\mathfrak{V}$. Therefore $\mathfrak{A}_1\mathfrak{V} \cap \mathfrak{A}_2\mathfrak{V} \leqq (\mathfrak{A}_1 \cap \mathfrak{A}_2)\mathfrak{V}$, and 8.10 follows.

We note that a similar argument will prove also $[\mathfrak{A}_1\mathfrak{V}, \mathfrak{A}_2\mathfrak{V}] = [\mathfrak{A}_1, \mathfrak{A}_2]\mathfrak{V}$; but we shall not make use of this. We sum up the preceding results in:

8.11. Theorem. *In the near-ring Φ_ω right multiplication by a fixed ideal $\mathfrak{V} \neq \{0\}$ constitutes an iso-endomorphism of the lattice of all ideals. This iso-endomorphism corresponds in F to the mapping of the lattice of all fully invariant subgroups, that is word subgroups, of F onto the sub-lattice of all word subgroups of the fully invariant subgroup B of F.*

An ideal of Φ_ω is a non-trivial product of two ideals if, and only if, the corresponding fully invariant subgroup of F is fully invariant in a proper fully invariant supergroup. We say:

8.12. Definition. *An ideal of Φ_ω is called indecomposable, if it is not the product of two proper ideals of Φ_ω.*

Examples of indecomposable ideals are all maximal ideals, but also, for instance, the derived ideal.

8.13. *Every ideal of Φ_ω is representable as a product of indecomposable ideals.*

Proof. If the ideal $\mathfrak{A}$ is not itself indecomposable, then $\mathfrak{A} = \mathfrak{B}_1\mathfrak{B}_2$. If at least one of the factors is not indecomposable, one factorizes further. That this process must break off after a finite number of steps, follows from Levi's theorem on chains of characteristic subgroups of a free group (cf. [7]): If $A = A_t < A_{t-1} < \cdots < A_0 = F$ is a chain of characteristic subgroups of F, and each term is characteristic in its successor, then the length t of the chain is at most equal to $l(A) - 2$, where $l(A)$ is the length (qua reduced word in F) of a shortest element of A. For this length $l(A_i)$ increases by at least 1 every time one descends from A_{i-1} to A_i in the chain.

A representation $\mathfrak{A} = \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_t$ of $\mathfrak{A}$ as a product of t factors leads to a chain of fully invariant subgroups of F, namely

$$A < B_2 \circ B_3 \circ \cdots \circ B_t < B_3 \circ \cdots \circ B_t < \cdots < B_{t-1} \circ B_t < B_t < F.$$

Every term is fully invariant, hence a fortiori characteristic, in its successor. It follows that t, that is the number of factors of $\mathfrak{A}$, is bounded by $\mathfrak{A}$ alone.

Nothing is known on the uniqueness, or otherwise, of a representation as a product of indecomposable factors. In fact it is not even sure that the left cancellation law holds in the semigroup of ideals. In the remainder of this paragraph we collect some partial results in this direction.

8.14. *If* $\mathfrak{A} \neq \boldsymbol{\Phi}_\omega$, $\{0\}$, *then* $\mathfrak{A}^{n+1} < \mathfrak{A}^n$ *for all* n, *and* $\bigcap_n \mathfrak{A}^n = \{0\}$.

Proof. Certainly $\mathfrak{A}^{n+1} \leqq \mathfrak{A}^n$. From $\mathfrak{A}^{n+1} = \mathfrak{A}\mathfrak{A}^n = \mathfrak{A}^n = \boldsymbol{\Phi}_\omega \mathfrak{A}^n$ follows $\mathfrak{A} = \boldsymbol{\Phi}_\omega$ by 8.09. Hence $\mathfrak{A}^{n+1} < \mathfrak{A}^n$. The fully invariant subgroup belonging to $\mathfrak{A}^{n+1}$ is fully invariant in that belonging to $\mathfrak{A}^n$. Hence, again by LEVI's theorem quoted above, the descending chain of these fully invariant subgroups contracts to $\{0\}$.

We deduce:

8.15. *If* $\mathfrak{B} \neq \{0\}$, *and* $\mathfrak{A}\mathfrak{B}\mathfrak{C} = \mathfrak{B}$, *then* $\mathfrak{A} = \mathfrak{C} = \boldsymbol{\Phi}_\omega$.

Proof. From $\mathfrak{A}\mathfrak{B}\mathfrak{C} = \mathfrak{B}$ one has inductively: $\mathfrak{A}^n\mathfrak{B}\mathfrak{C}^n = \mathfrak{B}$ for all n. Hence $\mathfrak{B} \leqq \mathfrak{A}^n \cap \mathfrak{C}^n$ for all n; thus, by 8.14, $\mathfrak{B} = \{0\}$ unless $\mathfrak{A} = \mathfrak{C} = \boldsymbol{\Phi}_\omega$.

Now 8.08, 8.09, and 8.15 give immediately:

8.16. *If* $\mathfrak{B}_1 \geqq \mathfrak{B}_2$, *and* B_2 *is fully invariant in* B_1, *then* $\mathfrak{A}\mathfrak{B}_1 = \mathfrak{A}\mathfrak{B}_2$ *with* $\mathfrak{A} \neq \{0\}$ *implies* $\mathfrak{B}_1 = \mathfrak{B}_2$.

A little more can be said, if $\mathfrak{B}_1$ and $\mathfrak{B}_2$ generate the whole of $\boldsymbol{\Phi}_\omega$. In that case, $\mathfrak{A}\mathfrak{B}_1 = \mathfrak{A}\mathfrak{B}_2$ can hold—if at all—only for an ideal $\mathfrak{A}$ which is contained in $\mathfrak{B}_1 \cap \mathfrak{B}_2$, and properly contained in the derived ideal.

8.17. *If* $\mathfrak{B}_1, \mathfrak{B}_2 \neq \boldsymbol{\Phi}_\omega$, $\mathfrak{B}_1 + \mathfrak{B}_2 = \boldsymbol{\Phi}_\omega$, *and* $\mathfrak{A}\mathfrak{B}_1 = \mathfrak{A}\mathfrak{B}_2$, *then* $\mathfrak{A} \leqq \mathfrak{B}_1 \cap \mathfrak{B}_2$.

Proof. By 7.12, we have $\mathfrak{A} = \mathfrak{A}(\mathfrak{B}_1 + \mathfrak{B}_2) \leqq \mathfrak{A}\mathfrak{B}_1 + \mathfrak{A}\mathfrak{B}_2 + (\mathfrak{A} \cap \mathfrak{B}_1 \cap \mathfrak{B}_2)$. Since $\mathfrak{A}\mathfrak{B}_1 \leqq \mathfrak{A} \cap \mathfrak{B}_1$, $\mathfrak{A}\mathfrak{B}_2 \leqq \mathfrak{A} \cap \mathfrak{B}_2$, it follows that $\mathfrak{A}\mathfrak{B}_1 = \mathfrak{A}\mathfrak{B}_2 \leqq \mathfrak{A} \cap \mathfrak{B}_1 \cap \mathfrak{B}_2$, hence $\mathfrak{A} \leqq \mathfrak{A} \cap \mathfrak{B}_1 \cap \mathfrak{B}_2$, which means $\mathfrak{A} \leqq \mathfrak{B}_1 \cap \mathfrak{B}_2$.

For the proof of the second statement above, we use the following

Notation: The derived ideal, that is the ideal corresponding to the derived group of F, is called $\mathfrak{D}$. The ideal corresponding to the fully invariant closure of the single word me_1, that is the fully invariant subgroup generated by all m^{th} multiples of elements of F, is called $\mathfrak{E}_m$.

8.18. *If* $\mathfrak{B}_1, \mathfrak{B}_2 \neq \boldsymbol{\Phi}_\omega$, $\mathfrak{B}_1 + \mathfrak{B}_2 = \boldsymbol{\Phi}_\omega$, *and* $\mathfrak{A}\mathfrak{B}_1 = \mathfrak{A}\mathfrak{B}_2$, *then* $\mathfrak{A} < \mathfrak{D}$.

Proof. If $\mathfrak{B}_1$ and $\mathfrak{B}_2$ together generate the whole of $\boldsymbol{\Phi}_\omega$, $\mathfrak{B}_1$ must contain $\mathfrak{E}_m$, and $\mathfrak{B}_2$ must contain $\mathfrak{E}_n$, for some integers m and n which are relative prime. We assume m and n to be as small as possible with these properties.

1. Assume $\mathfrak{A}$ contains elements outside the ideal $\mathfrak{D}$. Then $\mathfrak{A}$ contains the ideal $\mathfrak{E}_p$ for some positive integer p; again we take p as small as possible. Then $\mathfrak{A}\mathfrak{B}_1$ contains $\mathfrak{E}_{mp}$, and $\mathfrak{A}\mathfrak{B}_2$ contains $\mathfrak{E}_{np}$, and in each case, mp and np respectively are the least integers with this property. As $p \neq 0$, $mp \neq np$, hence $\mathfrak{A}\mathfrak{B}_1 \neq \mathfrak{A}\mathfrak{B}_2$ contrary to our assumption. Incidentally, in this case only $m \neq n$ has been used.

2. It remains to consider the case $\mathfrak{A} = \mathfrak{D}$. Here it suffices to show that $\mathfrak{D}\mathfrak{B}_1 + \mathfrak{D}\mathfrak{B}_2 = \mathfrak{D}$. For then $\mathfrak{D}\mathfrak{B}_1 = \mathfrak{D}\mathfrak{B}_2$ implies $\mathfrak{D}\mathfrak{B}_1 = \mathfrak{D}\mathfrak{B}_2 = \mathfrak{D}$, hence $\mathfrak{B}_1 = \mathfrak{B}_2 = \boldsymbol{\Phi}_\omega$ by 8.15, contrary to our assumptions.

Now $\mathfrak{E}_m \subseteq \mathfrak{V}_1$, and $\mathfrak{E}_n \subseteq \mathfrak{V}_2$, hence $\mathfrak{D}\mathfrak{E}_m + \mathfrak{D}\mathfrak{E}_n \subseteq \mathfrak{D}\mathfrak{V}_1 + \mathfrak{D}\mathfrak{V}_2$. Therefore it is sufficient to prove:

8.19. *If the integers m and n are relative prime, then* $\mathfrak{D}\mathfrak{E}_m + \mathfrak{D}\mathfrak{E}_n = \mathfrak{D}$.

Proof[8]). In terms of the corresponding fully invariant subgroups of F, 8.19 states that the derived groups of the fully invariant subgroups of F which are generated by all m^{th} multiples, and all n^{th} multiples of elements of F respectively, together generate the whole derived group of F. This will be proved by showing: Any group H, in which all m^{th} multiples permute with each other, and all n^{th} multiples permute with each other, where m and n are relative prime, is an abelian group.

Under the assumptions, the m^{th} multiples of elements of H generate an abelian normal subgroup M of H. The factor group H/M is of exponent m; therefore every element of H/M is an n^{th} multiple, as m is prime to n. But n^{th} multiples commute in H, and a fortiori also in H/M. Thus H/M is abelian, and M contains the derived group H_1 of H. By symmetry, H_1 is also contained in the normal subgroup N of H generated by all n^{th} multiples of elements of H, and so $H_1 \subseteq M \cap N$. But $M \cap N$ consists of elements permuting with both, all m^{th} and all n^{th} multiples, and these are in the centre of H, as every element h of H can be written in the form $h = r(mh) + s(nh)$ for suitable integers r and s. Hence the derived group belongs to the centre. If now $c = [a, b]$ is any commutator of H, then $[pa, qb] = pqc$ for all integers p and q. But $0 = [ma, mb] = m^2c$, and $0 = [na, nb] = n^2c$. Since m and n are relative prime, $c = 0$ follows, and so H is abelian.

Theorem 8.11 permits us to extend the results 8.17 and 8.18 slightly, without much significance for our knowledge of the semigroup of ideals of Φ_ω.

The obvious question whether there exist representations of ideals, or of indecomposable ideals, as intersections of larger ideals also remains unanswered. The missing distributive law, but more than that, the absence of a descending chain condition, and the lack of knowledge on ascending chain conditions make it doubtful that this approach befits the problem.

9. The relation between ideal multiplication in Φ_n and Φ_ω

We use the same nomenclature as in § 2: If $\mathfrak{A}$ is an ideal of Φ_ω, or of Φ_n, the intersection of $\mathfrak{A}$ with the sub-near-ring Φ_m $(n > m)$ is an ideal of Φ_m, which we call the restriction of $\mathfrak{A}$ to Φ_m. Similarly, if $\mathfrak{A}$ is an ideal in Φ_m, the ideal generated by $\mathfrak{A}$ in Φ_n, or in Φ_ω, is the extension of $\mathfrak{A}$ to Φ_n, or to Φ_ω, respectively. These notions correspond, of course, exactly to those used in § 2:

9.01. *The fully invariant subgroup belonging to the restriction (extension) of an ideal is the restriction (extension) of the fully invariant subgroup belonging to that ideal.*

---

[8]) This proof is due to my husband.

Hence, the statements 2.02 to 2.06 which govern these processes of restriction and extension hold, mutatis mutandis, for ideals in the near-rings.

Notation. If $\mathfrak{A}$ is an ideal of Φ_ω, its restriction to Φ_n is denoted by $\mathfrak{A}_n$, $\mathfrak{A}_n = \mathfrak{A} \cap \Phi_n$. The extension of $\mathfrak{A}_n$ to Φ_ω is denoted by $\mathfrak{A}^{(n)}$.

We summarize the facts we are going to use here:

9.02. *The ideals $\mathfrak{A}^{(n)}$ of Φ_ω form an ascending chain,*

$$\mathfrak{A}^{(1)} \subseteq \mathfrak{A}^{(2)} \subseteq \cdots \subseteq \mathfrak{A}^{(n)} \subseteq \cdots \subseteq \mathfrak{A}.$$

Here $\mathfrak{A}^{(n)} = \mathfrak{A}$ if, and only if, $\mathfrak{A}$ can be generated by elements of Φ_n. The ideals $\mathfrak{A}$ and $\mathfrak{A}^{(n)}$ have the same restriction $\mathfrak{A}_n$ to Φ_n.

To form the restriction $\mathfrak{A}_n$ of $\mathfrak{A}$ to Φ_n, we may use the relative identity element ε_n to pick out, as in 5.03, that part of $\mathfrak{A}$ that lies in Φ_n:

$$\mathfrak{A}_n = \mathfrak{A} \cap \Phi_n = \mathfrak{A} \cap \varepsilon_n \Phi_\omega \varepsilon_n = \varepsilon_n \mathfrak{A} \varepsilon_n.$$

In particular:

9.03. *The restriction $(\mathfrak{A}\mathfrak{B})_n$ of the product $\mathfrak{A}\mathfrak{B}$ to Φ_n consists of all elements of the form $(\varepsilon_n \alpha)(\beta \varepsilon_n)$ with $\alpha \in \mathfrak{A}$, $\beta \in \mathfrak{B}$.*

For, by 7.16, $\mathfrak{A}\mathfrak{B}$ consists of all products $\alpha\beta$, $\alpha \in \mathfrak{A}$, $\beta \in \mathfrak{B}$; hence $\mathfrak{A}\mathfrak{B} \cap \Phi_n = \varepsilon_n \mathfrak{A}\mathfrak{B} \varepsilon_n$ consists of all products $\varepsilon_n \alpha \beta \varepsilon_n$. The factor $\varepsilon_n \alpha$ is an element with at most n non-trivial components, which belong to A. The second factor $\beta \varepsilon_n$ is an element whose components belong to F_n, that is, to $B \cap F_n = B_n$; the number of non-trivial components may, of course, be greater than n. But as $B_n < B^{(n)}$, we always have:

9.04. *If $\beta \in \mathfrak{B}$, then $\beta \varepsilon_n \in \mathfrak{B}^{(n)}$.*

It follows:

9.05. *For any two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of Φ_ω,*

$$\mathfrak{A}\mathfrak{B} \supseteq \mathfrak{A} \cdot \mathfrak{B}^{(n)} \supseteq (\mathfrak{A}\mathfrak{B})^{(n)},$$

and the restriction to Φ_n of all three terms is the same ideal of Φ_n.

Proof. As $\mathfrak{B}^{(n)} \subseteq \mathfrak{B}$, clearly $\mathfrak{A}\mathfrak{B}^{(n)} \subseteq \mathfrak{A}\mathfrak{B}$. Also, $(\mathfrak{A}\mathfrak{B})^{(n)}$ is the ideal generated in Φ_ω by the restriction of $\mathfrak{A}\mathfrak{B}$ to Φ_n; hence 9.03 shows that it is generated by all elements of the form $(\varepsilon_n \alpha)(\beta \varepsilon_n)$. But $\varepsilon_n \alpha \in \mathfrak{A}$, $\beta \varepsilon_n \in \mathfrak{B}^{(n)}$ by 9.04, hence every generator of $(\mathfrak{A}\mathfrak{B})^{(n)}$ belongs to $\mathfrak{A}\mathfrak{B}^{(n)}$, and so $(\mathfrak{A}\mathfrak{B})^{(n)} \subseteq \mathfrak{A}\mathfrak{B}^{(n)}$. Further, by 9.02, $\mathfrak{A}\mathfrak{B}$ and $(\mathfrak{A}\mathfrak{B})^{(n)}$ have the same restriction to Φ_n, therefore the same is true for any ideal between these two.

9.06. *The restriction of $\mathfrak{A}^{(n)} \cdot \mathfrak{B}$ to Φ_n is the product $\mathfrak{A}_n \mathfrak{B}_n$ in Φ_n,*

$$\mathfrak{A}^{(n)} \mathfrak{B} \cap \Phi_n = \mathfrak{A}_n \mathfrak{B}_n.$$

Proof. As $\mathfrak{A}_n < \mathfrak{A}^{(n)}$ and $\mathfrak{B}_n < \mathfrak{B}$, $\mathfrak{A}_n \mathfrak{B}_n \subseteq \mathfrak{A}^{(n)} \mathfrak{B}$; the product $\mathfrak{A}_n \mathfrak{B}_n$ trivially belongs to Φ_n, hence $\mathfrak{A}_n \mathfrak{B}_n \subseteq \mathfrak{A}^{(n)} \cdot \mathfrak{B} \cap \Phi_n$. To prove the reverse inclusion, we note that $\mathfrak{A}^{(n)}$ is generated by $\mathfrak{A}_n$ in Φ_ω; hence, by 7.05, $\mathfrak{A}^{(n)}$ consists of all elements of the form $\sum \xi \alpha_n \eta$, where $\alpha_n \in \mathfrak{A}_n$ and $\xi, \eta \in \Phi_\omega$. Therefore, by 7.16, $\mathfrak{A}^{(n)}\mathfrak{B}$ consists of all elements of the form $\gamma = (\sum \xi \alpha_n \eta)\beta$.

Here $\alpha_n = \varepsilon_n \alpha_n \varepsilon_n$, as $\alpha_n \in \boldsymbol{\Phi}_n$. If now the element γ belongs also to $\boldsymbol{\Phi}_n$, then $\gamma = \varepsilon_n \gamma \varepsilon_n$. Hence, $\gamma \in \mathfrak{A}^{(n)} \mathfrak{B} \cap \boldsymbol{\Phi}_n$ implies:

$$\begin{aligned} \gamma &= \varepsilon_n (\sum \xi \varepsilon_n \alpha_n \varepsilon_n \eta) \beta \varepsilon_n \\ &= \sum \varepsilon_n \xi \varepsilon_n \cdot \alpha_n \cdot \varepsilon_n \eta \beta \varepsilon_n \qquad \text{by 5.04,} \\ &= \sum \xi_n \alpha_n \beta_n, \qquad \text{where} \qquad \xi_n \in \boldsymbol{\Phi}_n, \beta_n \in \varepsilon_n \mathfrak{B} \varepsilon_n = \mathfrak{B}_n. \end{aligned}$$

Hence $\gamma \in \mathfrak{A}_n \mathfrak{B}_n$, which was to be proved.

Now 9.05, applied to $\mathfrak{A}^{(n)}$ in place of $\mathfrak{A}$ gives:

9.07. *For any two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of $\boldsymbol{\Phi}_\omega$,*

$$\mathfrak{A}^{(n)} \mathfrak{B} \geqq \mathfrak{A}^{(n)} \mathfrak{B}^{(n)} \geqq (\mathfrak{A}_n \mathfrak{B}_n)^{(n)},$$

and the restriction of all three terms to $\boldsymbol{\Phi}_n$ is the same ideal $\mathfrak{A}_n \mathfrak{B}_n$.

This shows that the restriction to $\boldsymbol{\Phi}_n$ of a product, whose first factor can be generated by elements involving at most n generators, is the product of the restrictions of the factors, irrespective of the nature of the second factor. The converse is not as straightforward: The rank $N(B_n)$ of the free subgroup B_n of F_n makes a difference to the situation. If $N = N(B_n)$ is finite, then, by SCHREIER's formula, $N \geqq n$; and $N = n$ only if $B_n = F_n$. Here we have excluded the trivial case $B_n = \{0\}$. Therefore, whether N is finite or infinite, we have $\mathfrak{A} \geqq \mathfrak{A}^{(N)} \geqq \mathfrak{A}^{(n)}$, hence also $\mathfrak{A}\mathfrak{B} \geqq \mathfrak{A}^{(N)} \mathfrak{B} \geqq \mathfrak{A}^{(n)} \mathfrak{B}$ [9]), and the restrictions of these products to $\boldsymbol{\Phi}_n$ are in the same relation to each other. We show first:

9.08. *If B_n is of finite rank N as free subgroup of F_n, then*

$$\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(N)} \mathfrak{B} \cap \boldsymbol{\Phi}_n.$$

Proof. The right-hand side is contained in the left-hand side, hence we need only prove that $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n \subseteq \mathfrak{A}^{(N)} \mathfrak{B} \cap \boldsymbol{\Phi}_n$.

Let $b_1, \ldots, b_N$ $(N \geqq n)$ be free generators of B_n, and let β_N denote the element of $\mathfrak{B}$ whose first N components are $b_1, \ldots, b_N$, and whose further components are zero. Then every element of $\mathfrak{B}$ whose components belong to B_n is representable in the form $\xi \beta_N$, where the components of ξ belong to F_N, that is $\xi = \xi \varepsilon_N$. If now $\gamma \in \mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n$, then $\gamma = (\varepsilon_n \alpha)(\beta \varepsilon_n)$ for some $\alpha \in \mathfrak{A}$ and $\beta \in \mathfrak{B}$. But $\beta \varepsilon_n$ has components in B_n, hence $\gamma = (\varepsilon_n \alpha)(\xi \beta_N)$, where ξ has components in F_N; thus $\gamma = (\varepsilon_n \alpha)(\xi \varepsilon_N \beta_N) = (\varepsilon_n \alpha \xi \varepsilon_N) \beta_N$. Since $\varepsilon_n \alpha \xi \in \mathfrak{A}$, 9.04 shows that $\varepsilon_n \alpha \xi \varepsilon_N \in \mathfrak{A}^{(N)}$; hence $\gamma \in \mathfrak{A}^{(N)} \mathfrak{B}$. But $\gamma \in \boldsymbol{\Phi}_n$, and so $\gamma \in \mathfrak{A}^{(N)} \mathfrak{B} \cap \boldsymbol{\Phi}_n$, which proves 9.08.

Now we can complete the picture by showing:

9.09. Theorem. *If $\mathfrak{A}$ and $\mathfrak{B} \neq \{0\}$ are ideals of $\boldsymbol{\Phi}_\omega$, where $B \cap F_n = B_n$ is of finite or infinite rank N as free subgroup of F_n, then the restriction to $\boldsymbol{\Phi}_n$ of the product $\mathfrak{A}\mathfrak{B}$ is the product of the restrictions of $\mathfrak{A}$ and $\mathfrak{B}$, $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}_n \mathfrak{B}_n$, if and only if, $\mathfrak{A}^{(N)} = \mathfrak{A}^{(n)}$.*

[9]) Here, and repeatedly further on, we use the natural convention: if N is infinite, then $\mathfrak{A}^{(N)} = \mathfrak{A}$.

Proof. If $\mathfrak{A}^{(N)} = \mathfrak{A}^{(n)}$, then 9.07 and 9.08 show that $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}_n \mathfrak{B}_n$.

Conversely, $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}_n \mathfrak{B}_n$ implies by 9.05, 9.07 and 9.08 that $\mathfrak{A}^{(N)}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(n)}\mathfrak{B} \cap \boldsymbol{\Phi}_n$. Since trivially $\mathfrak{A}^{(n)} \leqq \mathfrak{A}^{(N)}$, all we have to show is:

$$\mathfrak{A}^{(N)}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(n)}\mathfrak{B} \cap \boldsymbol{\Phi}_n \quad \text{implies} \quad \mathfrak{A}^{(N)} \leqq \mathfrak{A}^{(n)}.$$

1. Assume N finite. As $\mathfrak{A}^{(N)}$ is generated by elements α whose components lie in F_N, it is sufficient to show that every such element α of $\mathfrak{A}^{(N)}$ belongs to $\mathfrak{A}^{(n)}$. We consider, for any such α, the product $\alpha\beta_N \in \mathfrak{A}^{(N)}\mathfrak{B}$, where β_N is the element of $\mathfrak{B}$ whose non-trivial components are the N free generators of B_n (as in the proof of 9.08). Then

$$\varepsilon_n(\alpha\beta_N)\,\varepsilon_n = (\varepsilon_n\alpha)\,\beta_N \in \mathfrak{A}^{(N)}\mathfrak{B} \cap \boldsymbol{\Phi}_n.$$

As $\mathfrak{A}^{(N)}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(n)}\mathfrak{B} \cap \boldsymbol{\Phi}_n$, there exist, by 9.03, elements $\alpha_1 \in \mathfrak{A}^{(n)}$ and $\beta_1 \in \mathfrak{B}$, such that $(\varepsilon_n\alpha)\beta_N = (\varepsilon_n\alpha_1)(\beta_1\varepsilon_n)$.

But $\beta_1\varepsilon_n$ has components in B_n, hence it is of the form $\beta_1\varepsilon_n = \xi\beta_N$, where the components of ξ lie in F_N; thus

$$(\varepsilon_n\alpha)\,\beta_N = (\varepsilon_n\alpha_1)\,(\xi\beta_N) = (\varepsilon_n\alpha_1\xi)\,\beta_N,$$

and this implies, by 8.03: $\varepsilon_n\alpha = \varepsilon_n\alpha_1\xi$.

Here $\varepsilon_n\alpha_1\xi$ lies in $\mathfrak{A}^{(n)}$, as α_1 belongs to $\mathfrak{A}^{(n)}$; hence the first n components of α, and therefore of every element of $\mathfrak{A}^{(N)}$ with components in F_N, belong to $A^{(n)}$. Since the components of the elements of an ideal vary independently over the corresponding fully invariant subgroup (cf. 6.05), every component of α belongs to $A^{(n)}$, and so $\alpha \in \mathfrak{A}^{(n)}$ as required.

2. Assume N infinite. We have to show:

$$\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(n)}\mathfrak{B} \cap \boldsymbol{\Phi}_n \quad \text{implies} \quad \mathfrak{A} \leqq \mathfrak{A}^{(n)}.$$

This time, let $b_1, b_2, \ldots$ be a set of free generators of B_n, and for every $m = 1, 2, \ldots$ denote by β_m the element of $\mathfrak{B}$ whose first m components are $b_1, \ldots, b_m$, and whose further components are zero. Consider any element $\alpha \in \mathfrak{A}$; the finitely many non-trivial components of α involve only a finite number of generators, $e_1, \ldots, e_k$ say. We consider the element $\alpha\beta_k$ of $\mathfrak{A}\mathfrak{B}$. Then $(\varepsilon_n\alpha)(\beta_k\varepsilon_n) = (\varepsilon_n\alpha)\beta_k$ is an element of $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n$. Since $\mathfrak{A}\mathfrak{B} \cap \boldsymbol{\Phi}_n = \mathfrak{A}^{(n)}\mathfrak{B} \cap \boldsymbol{\Phi}_n$, there exist elements $\alpha_1 \in \mathfrak{A}^{(n)}$, $\beta_1 \in \mathfrak{B}$, such that $(\varepsilon_n\alpha)\beta_k = (\varepsilon_n\alpha_1)(\beta_1\varepsilon_n)$. Again, $\beta_1\varepsilon_n$ has components in B_n, hence is of the form $\beta_1\varepsilon_n = \xi\beta_m$ for some m, where ξ has components in F_m. Therefore $(\varepsilon_n\alpha)\beta_k = (\varepsilon_n\alpha_1)(\xi\beta_m) = (\varepsilon_n\alpha_1\xi)\beta_m$, which implies by 8.03, $\varepsilon_n\alpha = \varepsilon_n\alpha_1\xi \in \mathfrak{A}^{(n)}$. As before, $\mathfrak{A} \leqq \mathfrak{A}^{(n)}$ follows.

We are now also in a position to answer the question raised by Theorem 7.19: In every near-ring $\boldsymbol{\Phi}_n$ or $\boldsymbol{\Phi}_\omega$, the fully invariant subgroup $A \circ B$ is fully invariant in B. In $\boldsymbol{\Phi}_\omega$, conversely, every fully invariant subgroup of B is of the form $A \circ B$ (Theorem 8.08). But in the near-rings $\boldsymbol{\Phi}_n$ this is not true. Instead we have:

9.10. Theorem. *If B_n and C_n are fully invariant subgroups of F_n, and $C_n \leqq B_n$, then C_n is fully invariant in B_n if, and only if, the corresponding ideal $\mathfrak{C}_n$ is the restriction to $\boldsymbol{\Phi}_n$ of an ideal product $\mathfrak{A}\mathfrak{B}^{(n)}$ in $\boldsymbol{\Phi}_\omega$. Moreover, if B_n is*

of finite rank N as free subgroup of F_n, then $\mathfrak{A} = \mathfrak{A}^{(N)}$ may be assumed. $\mathfrak{C}_n$ is itself a product in Φ_n if, and only if, $\mathfrak{A}^{(N)} = \mathfrak{A}^{(n)}$, and then $\mathfrak{C}_n = \mathfrak{A}_n \mathfrak{B}_n$, that is $C_n = A_n \circ B_n$.

Proof. If $\mathfrak{C}_n = \mathfrak{A}\mathfrak{B}^{(n)} \cap \Phi_n$, then C_n consists, by 9.03, of the components of all elements of the form $(\varepsilon_n \alpha)(\beta \varepsilon_n)$; that is, C_n consists of all "values" of the words in A for "arguments" in B_n. Thus C_n is a word subgroup, that is a fully invariant subgroup of B_n.

Conversely, if C_n is fully invariant in B_n, it is a word subgroup of B_n; there exists, therefore, a set of words $a_i(b_1, b_2, \ldots)$ in the free generators of B_n, such that C_n is the fully invariant closure of this set in B_n. We denote the fully invariant closure in F of the corresponding set of words $a_i(e_1, e_2, \ldots)$ by A. If B_n is of finite rank N, the words a_i are words in $b_1, \ldots, b_N$, hence A is the closure of the words $a_i(e_1, \ldots, e_N)$; therefore the corresponding ideal $\mathfrak{A}$ of Φ_ω satisfies $\mathfrak{A} = \mathfrak{A}^{(N)}$. Moreover, using again 9.03, one confirms easily, that with this choice of $\mathfrak{A}$, $\mathfrak{A}\mathfrak{B}^{(n)} \cap \Phi_n = \mathfrak{C}_n$.

The remaining statements of the theorem now follow from 9.08 and 9.09.

In conclusion, we return to the non-associativity of ideal multiplication in the near-rings Φ_n: we have yet to confirm by an example, that the associative law may, in fact, be violated. The situation is now clear:

If $\mathfrak{A}_n$, $\mathfrak{B}_n$, $\mathfrak{C}_n$ are any three ideals in Φ_n, and $\mathfrak{A}^{(n)}$, $\mathfrak{B}^{(n)}$, $\mathfrak{C}^{(n)}$ their extensions to Φ_ω, then in Φ_ω, $\mathfrak{A}^{(n)}(\mathfrak{B}^{(n)}\mathfrak{C}^{(n)}) = (\mathfrak{A}^{(n)}\mathfrak{B}^{(n)})\mathfrak{C}^{(n)}$. Also, from 9.07, $\mathfrak{A}^{(n)}\mathfrak{B}^{(n)} \cap \Phi_n = \mathfrak{A}_n \mathfrak{B}_n$ and $\mathfrak{B}^{(n)}\mathfrak{C}^{(n)} \cap \Phi_n = \mathfrak{B}_n \mathfrak{C}_n$, hence $\mathfrak{A}_n(\mathfrak{B}_n \mathfrak{C}_n) = \mathfrak{A}^{(n)}(\mathfrak{B}^{(n)}\mathfrak{C}^{(n)}) \cap \Phi_n = (\mathfrak{A}^{(n)}\mathfrak{B}^{(n)})\mathfrak{C}^{(n)} \cap \Phi_n \supseteq (\mathfrak{A}_n \mathfrak{B}_n)^{(n)} \cdot \mathfrak{C}^{(n)} \cap \Phi_n = (\mathfrak{A}_n \mathfrak{B}_n)\mathfrak{C}_n$. Although $\mathfrak{A}^{(n)}$ and $\mathfrak{B}^{(n)}$ both are generated by elements in Φ_n, their product need not have this property, and in that case the inclusion $(\mathfrak{A}_n \mathfrak{B}_n)^{(n)} \subset \mathfrak{A}^{(n)}\mathfrak{B}^{(n)}$ is proper. If then further the group C_n corresponding to $\mathfrak{C}_n$ is of infinite rank, 9.09 shows that

$$(\mathfrak{A}_n \mathfrak{B}_n)\mathfrak{C}_n \subset \mathfrak{A}_n(\mathfrak{B}_n \mathfrak{C}_n).$$

9.11. Example. We take $n = 2$, and $\mathfrak{A}_2 = \mathfrak{B}_2 = \mathfrak{C}_2$ all as the derived ideal $\mathfrak{D}_2$ of Φ_2. Then $\mathfrak{D}^{(2)}$ is the derived ideal of Φ_ω. Hence: $\mathfrak{D}^{(2)} \cdot \mathfrak{D}^{(2)}$ is the second derived ideal of Φ_ω. (The associated second derived group was denoted by A in Example 2.11, which we shall use here.) $\mathfrak{D}_2\mathfrak{D}_2$ is the second derived ideal of Φ_2, so that $(\mathfrak{D}_2\mathfrak{D}_2)^{(2)}$ is the ideal of Φ_ω corresponding to the two-variable metabelian laws, which, by 2.12, is properly contained in the second derived ideal of Φ_ω:

$$(\mathfrak{D}_2\mathfrak{D}_2)^{(2)} \subset \mathfrak{D}^{(2)}\mathfrak{D}^{(2)}.$$

Since, moreover, the derived group of F_2 is of infinite rank, we have:

9.12. *In Φ_2,* $\quad (\mathfrak{D}_2\mathfrak{D}_2)\mathfrak{D}_2 \subset \mathfrak{D}_2(\mathfrak{D}_2\mathfrak{D}_2)$,

showing that ideal multiplication in Φ_2 is not power associative.

The fully invariant subgroup of F_2 corresponding to the right-hand side of 9.12 is simply the third derived group—obtained as the derived group of the second derived group. The group corresponding to the left-hand side of 9.12

is the two-variable second derived group of the derived group, properly contained in the third derived group—the latter this time thought of as the whole second derived group of the derived group.

10. Appendix: Ideal bases

The elements α_i form a basis for the ideal $\mathfrak{A}$ in Φ_n or Φ_ω, if, and only if, their components form a basis for the corresponding fully invariant subgroup A in F_n or F respectively. In particular, $\mathfrak{A}$ is finitely based if, and only if, A is finitely based. In the free group F of infinite rank, a single word is sufficient to generate A, whenever A is finitely based. The corresponding ideal, generated by a single element, may be reasonably called a principal ideal.

Problem. *Is the product of two principal ideals of Φ_ω necessarily finitely based, that is, itself a principal ideal?*

An infinite ideal basis for such a product can easily be given: If A is the closure in F of the word $a(e_1, \ldots, e_m)$, and B is the closure in F of the word $b(e_1, \ldots, e_n)$, we put

$$a_r = a(e_1 + \cdots + e_r, e_{r+1} + \cdots + e_{2r}, \ldots, e_{(m-1)r+1} + \cdots + e_{mr}),$$

and we take β_r as the "matrix"

$$\beta_r = \begin{pmatrix} b(e_1, \ldots, e_n) \\ b(e_{n+1}, \ldots, e_{2n}) \\ \cdots\cdots\cdots\cdots \\ b(e_{(mr-1)n+1}, \ldots, e_{mrn}) \end{pmatrix},$$

all further components being zero. Then:

10.01. *The elements $c_r = a_r \beta_r$, $r = 1, 2, \ldots$, form a basis for $A \circ B$. Every finite subset of this basis is redundant, as c_r is obtained from c_{r+1} by substituting zeros for some of the generators e_i.*

In special cases, this infinite basis can be reduced to a single element. We give two examples:

10.02. Example. $A = \{2e_1\}$, $B = \{2e_1\} = A$; that is, $A \circ B = A \circ A$ is the "square" of the word group generated by all doubles of elements of F. Here $c_r = 2(2e_1 + \cdots + 2e_r)$. Using that every commutator is a sum of doubles, one shows inductively: $c_r \in \{c_{r-1}\}$ for $r \geq 3$. Therefore

$A \circ A$ is the closure of the single word $2(2e_1 + 2e_2)$.

10.03. Example. $A = \{2e_1\}$, $B = \{3e_1\}$. Here the basis 10.01 for $A \circ B$ consists of the elements $c_r = 2(3e_1 + \cdots + 3e_r)$, $r = 1, 2, \ldots$, and the basis 10.01 for $B \circ A$ consists of the elements $d_r = 3(2e_1 + \cdots + 2e_r)$, $r = 1, 2, \ldots$. In the first case, an argument similar to the one used in Example 10.02 shows that the single word $2(3e_1 + 3e_2)$ is sufficient; in the second case, GRAHAM HIGMAN has shown[10]) that there exists an integer k such that d_r with $r > k$ follows from d_k. Thus:

[10]) Unpublished.

$A \circ B$ is the closure of $2(3e_1+3e_2)$, $B \circ A$ is the closure of $3(2e_1+\cdots+2e_k)$ for some integer k.

In connection with this last example, HIGMAN conjectured that $A \circ B$ is finitely based, whenever A contains some term of the lower central series of F.

Finally, these examples suggest a further question; in § 2 we denoted by $k = k(A)$ the least integer such that A is the closure of a set of words involving at most k variables.

Problem. *Is $k(A \circ B)$ finite, provided $k(A)$ and $k(B)$ are finite? And if the answer is positive, can one give a bound for $k(A \circ B)$ in terms of $k(A)$ and $k(B)$?*

Bibliography

[*1*] BAER, R.: Groups with proper isomorphic quotient groups. Bull. Amer. Math. Soc. **50**, 267—278 (1944). — [*2*] BLACKETT, D. W.: Simple and semi-simple near-rings. Proc. Amer. Math. Soc. **4**, 772—785 (1953). — [*3*] DESKINS, W. E.: A radical for near-rings. Proc. Amer. Math. Soc. **5**, 825—827 (1954). — [*4*] ETHERINGTON, I. M. H.: Non-associative arithmetics. Proc. Roy. Soc. Edinburgh, Sect. A **62**, 442—453 (1949). — [*5*] GRUENBERG, K.: Unpublished. — [*6*] HALL, P.: The splitting properties of relatively free groups. Proc. London Math. Soc. (3) **4**, 343—356 (1954). — [*7*] LEVI, F.: Über die Untergruppen der freien Gruppen. 2. Mitteilung. Math. Z. **37**, 90—97 (1933). — [*8*] LEVI, F., and B. L. VAN DER WAERDEN: Über eine besondere Klasse von Gruppen. Abh. math. Sem. Hans. Univ. **9**, 154—158 (1932). — [*9*] LYNDON, R. C.: Two notes on nilpotent groups. Proc. Amer. Math. Soc. **3**, 579—583 (1952). — [*10*] MAGNUS, W.: Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. Math. Ann. **111**, 259—280 (1935). — [*11*] NEUMANN, B. H.: Identical relations in groups. I. Math. Ann. **114**, 506—525 (1937). — [*12*] NEUMANN, B. H.: On a problem of Hopf. J. London Math. Soc. **28**, 351—353 (1953). — [*13*] ROBINSON, A.: On non-associative systems. Proc. Edinburgh Math. Soc. (2) **8**, 111—119 (1949). [*14*] WEVER, F.: Über Regeln in Gruppen. Math. Ann. **122**, 334—339 (1950). — [*15*] ZASSENHAUS, H.: Gruppentheorie, pp. 71—74. 1937.

Department of Mathematics, The University, Hull (England)

(Eingegangen am 9. Oktober 1955)

Foster, A. L.
Math. Zeitschr. Bd. 65, S. 70—75 (1956)

Ideals and their Structure in Classes of Operational Algebras

By
Alfred L. Foster

1. Introduction

In the realm of Boolean algebras the classical ideal structure theorem (Stone [1])[1]) asserts: *In a Boolean algebra each (non-unit) ideal is the intersection of its prime ideal — or equivalently, of its maximal ideal — divisors.*

Intimately related to this stands the fundamental subdirect structure theorem: *Each Boolean algebra is isomorphic with a subdirect power of the 2-element Boolean algebra.* A parallel subdirect structure is known for p-rings (McCoy and Montgomery [2], Foster [7]) and again for Post algebras (Rosenbloom [4], Wade [5], Foster [7]).

On a considerably broader front, in a series of recent papers dedicated to the development of a general "Boolean" theory of operational (or universal) algebras (Foster [7] to [12]), it was shown that the entire range of classical Boolean theory — e.g., duality principle, associated "logic", normal expansion theorem (for Boolean functions), structure theory, etc. — may be lifted, in generalized form, to a variety of successively more comprehensive universal algebra levels. Viewed from such a vantage point the Boolean-, Post- and p-ring theories, in particular, emerge as quite special instances of the extended theory.

In the present brief communication our concern is essentially limited to structure theory on the universal algebra level; specifically, we shall transform the two structure theorems of [7] and [8] — both of which are "subdirect" results — to "maximal-ideal" form, corresponding to (and generalizing) the classical Boolean structure theorem of Stone.

2. Some basic notions

In this section we recall several pertinent basic concepts and results of [7], [8]. Let $\mathfrak{A} = (A, o_1, o_2, \ldots)$ be a universal algebra of species $Sp = (n_1, n_2, \ldots)$, that is, an algebra whose basic operations o_i are n_i-ary $(i = 1, 2, \ldots)$. $\mathfrak{A}$ is called *functionally (strictly) complete* (f.s.c.) if for each $k = 1, 2, \ldots$ each set-theoretic mapping $f(\xi_1, \xi_2, \ldots, \xi_k)$ of the class $A \times A \times \cdots$ (k^{th} Cartesian power) into the set A is representable in at least one way as a *(strict) $\mathfrak{A}$-function*, i.e., as some composition, via the primitive operations o_i, of indeterminates

[1]) Square brackets refer to the appended bibliography.

$\xi_1, \ldots, \xi_k$ over A. The one-element algebra (of any species), denoted by $\overset{\circ}{|}$, is of course f.s.c. *A primal* algebra (of given species) is defined as a f.s.c. algebra $\neq \overset{\circ}{|}$. Among the properties of such algebras are the following, selected from [7], [8]:

Theorem 1. Let $\mathfrak{P} = (P, o, \ldots)$ *be a primal algebra of species* $Sp = (n_1, n_2, \ldots)$. *Then:*

(1) *There exists at least one* n_i *of* Sp *such that* $n_i > 1$.

(2) $\mathfrak{P}$ *is a finite algebra (i.e.,* P *is a finite class).*

(3) $\mathfrak{P}$ *is simple (i.e., possesses no proper ideals).*

(4) $\mathfrak{P}$ *possesses no subalgebra (except* $\mathfrak{P}$ *itself).*

(5) *The class of strict identities of* $\mathfrak{P}$ *is a maximal class*[2]).

(6) *The class of strict identities of* $\mathfrak{P}$ *possesses a finite basis*[3]).

For each species [subject to (1) of theorem 1] and for each integer $n > 1$, there exists at least one primal algebra of n elements (= *order* n). Illustrative of the profusion of such algebras we recall the following classes of primals ([7], [8]):

(a) $(F_2, \times, ^{\circ})$, the 2-element Boolean algebra ($\times$ = intersection, $^{\circ}$ = complement).

More generally

(b) $(F_p, \times, ^{\circ})$, the prime field, where: $\xi \times \eta$ is the product, and $\xi^{\circ} = 1 + \xi$ in the prime field $(F_p, \times, +)$.

(c) $(\mathcal{F}_n, \times, ^{\circ})$, the "$n$-field", where: $\mathcal{F}_n = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2}\}$, $\mathcal{F}_n' = \mathcal{F}_n$ less 0, $(\mathcal{F}_n', \times)$ = cyclic group of order $n-1$ $(\alpha^{n-1} = 1)$,

$$0 \times \xi = \xi \times 0 = 0 \,(\xi \in \mathcal{F}),\ \xi^{\circ} = \text{def}: 0^{\circ} = 1, 1^{\circ} = \alpha,\ \alpha^{\circ} = \alpha^2, \ldots, (\alpha^{n-2})^{\circ} = 0.$$

If the (arbitrary) integer n is chosen as a prime power we have to do with a simple form of the corresponding Galois field. More generally,

(d) $(G_n, \times, ^{\circ})$, an "ordered group with null", where: $G_n = \{0, 1, \alpha, \beta, \ldots\}$, $G_n' = G_n$ less 0, $(G_n', \times)$ = arbitrary group of order $n-1$ (with 1 as its identity), $\xi^{\circ} = \text{def}$ = arbitrary cyclic permutation of the elements of G_n, $0 \times \xi = \xi \times 0 = 0 \,(\xi \in G_n)$.

(e) $(P_n, \times, ^{\circ})$, the basic Post-algebra of order n, where:

$$P_n = \{0, \alpha_{n-2}, \alpha_{n-1}, \ldots, \alpha_2, \alpha_1, 1\}, \qquad \xi \times \eta = \min(\xi, \eta)$$

where "min" refers to the above sequence as "ascending", $\xi^{\circ} = \text{def}$:

$$0^{\circ} = 1,\ 1^{\circ} = \alpha_1,\ \alpha_1^{\circ} = \alpha_2, \ldots, (\alpha_{n-2})^{\circ} = 0.$$

Additional classes of primal algebras are found in [7], [8].

---

[2]) A strict identity $f(\xi, \ldots) = g(\xi, \ldots)$ of an algebra $\mathfrak{P}$ is one in which f and g are both strict $\mathfrak{P}$-functions. "Maximal" here means: from the strict identities of $\mathfrak{P}$, augmented by any single strict equation (of species Sp) which is not an identity of $\mathfrak{P}$, any desired equation (of species Sp) is logically deducible.

[3]) This finite basis result, [6], while implicit in [7], was first explicitly proved by YAQUB, [13].

3. $\mathfrak{P}$-algebras; sub-direct structure

Let $\mathfrak{P}$ be an arbitrary but fixed primal algebra, and let Sp denote its species. An algebra $\mathfrak{A}$ of species Sp is called a *$\mathfrak{P}$-algebra*, or an algebra with *kernel* $\mathfrak{P}$, if $\mathfrak{A}$ satisfies all strict identities of $\mathfrak{P}$ (see earlier footnote). Equivalently stated, the class of $\mathfrak{P}$-algebras may be defined as the class of algebras, of species Sp, which satisfy a certain finite list $I_1, I_2, \ldots, I_t$ of strict equations; here $I_1, \ldots, I_t$ may be chosen as any finite basis for the strict identities of the kernel, $\mathfrak{P}$ [compare with (6) of theorem 1].

In particular the class of algebras with: (a), kernel $(F_2, \times, ^{\circ})$ is identified as the class of Boolean algebras; (b) kernel $(F_p, \times, ^{\circ})$ is coextensive with the class of p-algebras (p-rings) (McCOY and MONTGOMERY [2], FOSTER [11], [12]; ...; (e), kernel $(P_n, \times, ^{\circ})$ is identical with the class of Post algebras of period n (ROSENBLOOM [4], WADE [5], FOSTER [7], [8], etc).

We shall require the following easy

Lemma 2. A homomorphic image of a $\mathfrak{P}$-algebra is a $\mathfrak{P}$-algebra.

Proof. Let $\mathfrak{A}$ be a $\mathfrak{P}$-algebra and $\mathfrak{B}$ a homomorphic image of $\mathfrak{A}$. Since the strict identities of any operational algebra are inherited by each of its homomorphic images, $\mathfrak{B}$ satisfies all strict identities of $\mathfrak{A}$ and therefore also of $\mathfrak{P}$. The lemma thus follows[4]).

We shall also need a section of the principal structure theorem proved in [7], namely

Theorem 3. Let $\mathfrak{P}$ be an arbitrary primal algebra. Then the three classes of algebras below are pairwise coextensive (up to isomorphisms):

(i) *The class of all $\mathfrak{P}$-algebras.*

(ii) *The class of all subdirect powers of $\mathfrak{P}$.*

(iii) *The class of all subalgebras of direct powers of $\mathfrak{P}$.*

Further, each finite $\mathfrak{P}$-algebra is isomorphic with a direct power of $\mathfrak{P}$.

4. Primal- and maximal-ideals; ideal structure

If $\mathfrak{B}$ is a universal algebra and $\mathfrak{I}$ an ideal of $\mathfrak{B}$, $\mathfrak{I}$ is called a *primal-ideal* if the factor algebra $\mathfrak{B}/\mathfrak{I}$ is a primal algebra.

Theorem 4. Let $\mathfrak{P}$ be a primal algebra and $\mathfrak{A}$ a $\mathfrak{P}$-algebra.

(i) *If $\mathfrak{I}$ is a primal ideal of $\mathfrak{A}$ then $\mathfrak{A}/\mathfrak{I} \cong \mathfrak{P}$.*

(ii) *A primal ideal of $\mathfrak{A}$ is a maximal ideal, and conversely.*

(iii) *If $\mathfrak{A} \neq \overset{\circ}{|}$ (= one-element algebra), then $\mathfrak{A}$ possesses at least one primal ideal.*

Proof. (i) We shall assume $\mathfrak{A} \neq \overset{\circ}{|}$ since in this case the theorem is vacuously true. Let $\mathfrak{I}$ be a primal ideal, whence $\mathfrak{A}/\mathfrak{I} \cong \mathfrak{Q}$ = primal algebra. Again $\mathfrak{Q}$, as homomorphic image of $\mathfrak{A}$, is a $\mathfrak{P}$-algebra (lemma 2). By theorem 3 the (finite) algebra $\mathfrak{Q}$ is then isomorphic with a direct power of $\mathfrak{P}$. This power could only be the first, i.e. $\mathfrak{Q} \cong \mathfrak{P}$, since otherwise the primal $\mathfrak{Q}$ would possess a proper ideal [(3) of theorem 1]. This proves (i).

[4]) Clearly the lemma does not require $\mathfrak{P}$ to be primal.

(ii) Let $\mathfrak{I}$ be a primal ideal of $\mathfrak{A}$. Then $\mathfrak{A}/\mathfrak{I} \cong \mathfrak{P}$, by part (i), and therefore $\mathfrak{I}$ is maximal; for if not, $\mathfrak{P}$ would possess a proper homomorphic image, contrary to (3) of theorem 1. Conversely, suppose $\mathfrak{I}$ is maximal. Then $\mathfrak{A}/\mathfrak{I}$, as homomorphic image of $\mathfrak{A}$, is a $\mathfrak{P}$-algebra (lemma 2), and $\mathfrak{A}/\mathfrak{I}$ is isomorphic with a subdirect power of $\mathfrak{P}$ (theorem 3). This subdirect power must be $\mathfrak{P}$ itself - whence $\mathfrak{A}/\mathfrak{I} \cong \mathfrak{P}$ and $\mathfrak{I}$ is a primal ideal —, for otherwise $\mathfrak{A}/\mathfrak{I}$ would possess a proper homomorphic image, contradicting the assumption that $\mathfrak{I}$ is maximal.

(iii) If $\mathfrak{A}$ is a primal algebra then 0, the null ideal of $\mathfrak{A}$, is a primal ideal since $\mathfrak{A}/0 \cong \mathfrak{A}$. Quite generally (theorem 3), $\mathfrak{A}$ is isomorphic with a subdirect power of $\mathfrak{P}$,

$$\alpha \in \mathfrak{A},\ \alpha = (\alpha_1, \ldots, \alpha_i, \ldots);\ \alpha_1 \in \mathfrak{P}, \ldots, \alpha_i \in \mathfrak{P}, \ldots$$

whence each ideal $\mathfrak{I}_i$, corresponding to the "natural" homomorphism $\alpha \to \alpha_i$, is clearly a primal ideal since $\mathfrak{A}/\mathfrak{I}_i \cong \mathfrak{P}$.

The first ideal-structure theorem is now given by

Theorem 5. Let $\mathfrak{P}$ be a primal algebra and $\mathfrak{A}$ a $\mathfrak{P}$-algebra. Then each non-unit ideal of $\mathfrak{A}$ is the intersection of its maximal (= primal) ideal divisors.

Proof. We again assume $\mathfrak{A} \neq \overset{c}{|}$ since in this case the theorem is vacuously true. As before let 0 be the null ideal of $\mathfrak{A}$, whence $\mathfrak{A}/0 \cong \mathfrak{A}$. We shall need the following theorem of Birkhoff [6], — see also McCoy [3]:

Theorem 6. Let $\{\ldots, \mathfrak{G}_i, \ldots\}$ be a class of universal algebras $\mathfrak{G}_i$, all of the same species. A necessary and sufficient condition for an algebra $\mathfrak{B}$ to be isomorphic with a subdirect product of the algebras $\mathfrak{G}_i$ is that $\mathfrak{B}$ possess a class $\{\ldots, \mathfrak{I}_i, \ldots\}$ of ideals, $\mathfrak{I}_i$, (1°) whose intersection is the null-ideal,

$$\cap \{\ldots, \mathfrak{I}_i, \ldots\} = 0,$$

and such that (2°) for the corresponding factor algebras,

$$\mathfrak{B}/\mathfrak{I}_i \cong \mathfrak{G}_i \qquad \textit{(for each index } i\textit{)}.$$

We return to the proof of theorem 5. Using one half of theorem 6 — with all $\mathfrak{G}_i$ taken as the same primal algebra, $\mathfrak{P}$ — and with due regard to theorem 3, it follows that: $\mathfrak{A}$ (or what is the same, the null ideal of $\mathfrak{A}$) is the intersection of a class $\{\ldots, \mathfrak{I}_i, \ldots\}$ of ideals $\mathfrak{I}_i$ such that

$$\mathfrak{A}/\mathfrak{I}_i \cong \mathfrak{P} \qquad \text{(for each index } i\text{)}.$$

It follows that these ideals $\mathfrak{I}_i$ are primal, and therefore maximal in $\mathfrak{A}$ (theorem 4).

Let now $\mathfrak{I}$ be an arbitrary ideal in $\mathfrak{A}$, and consider the factor algebra

$$\mathfrak{B} = \text{def} = \mathfrak{A}/\mathfrak{I}.$$

By lemma 2, $\mathfrak{B}$ is again a $\mathfrak{P}$-algebra and therefore by the foregoing conclusion (with $\mathfrak{B}$ replacing $\mathfrak{A}$) we have: $\mathfrak{B}$ (or the null ideal of $\mathfrak{B}$) is expressible as the intersection of a class of maximal ideals in $\mathfrak{B}$. Now, in an obvious way, to each ideal of the factor algebra $\mathfrak{B}$ corresponds an ideal in $\mathfrak{A}$, and in this correspondence: (1) to the null ideal of $\mathfrak{B}$ corresponds the ideal $\mathfrak{I}$ of $\mathfrak{A}$,

and (2) to a maximal ideal of $\mathfrak{B}$ corresponds a maximal ideal of $\mathfrak{A}$. Hence the ideal $\mathfrak{I}$ of $\mathfrak{A}$ is expressible as the intersection of a class of maximal ideals of $\mathfrak{A}$. Thus $\mathfrak{I}$ is the intersection of all its maximal ideal divisors, and theorem 5 is proved.

5. *The second ideal structure theorem*

The concept $\mathfrak{P}$-algebra is perforce based on a single (primal) algebra as kernel. In [8] a multiple-kernel theory was initiated, where such a kernel now consists of an appropriately selected class of primal algebras. We shall briefly recall a pertinent segment of this theory.

Algebras $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k$, all of the same species Sp,

$$\mathfrak{A}_i = (A_i, o, \ldots)$$

are said to be *strictly independent* if, corresponding to each given set (sequence) of k expressions of species Sp,

$$\Phi_1(\xi, \ldots), \ \Phi_2, \ldots, \Phi_k$$

there exists at least one fixed expression $\chi(\xi, \ldots)$ such that

$$\Phi_i(\xi, \ldots) = \chi(\xi, \ldots) \pmod{\mathfrak{A}_i}, \qquad (i = 1, 2, \ldots, k). \tag{5.1}$$

Here an *expression* is simply one or more indeterminante symbols $\xi, \ldots$ combined via the primitive operations $o, \ldots$ of Sp; in each algebra $\mathfrak{A}$ of species Sp, a given expression represents a strict $\mathfrak{A}$-function. Further, (5.1) is to be read: $\Phi_i = \chi$ is a (strict) identity of the algebra $\mathfrak{A}_i$.

Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_k$ $(k \geqq 1)$ be a finite set of independent primal algebras, all of a given species Sp. An algebra $\mathfrak{A}$ of species Sp is said to be

Def 1. A $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$-*algebra* if $\mathfrak{A}$ satisfies all strict identities common to $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$, — or, equivalently, if $\mathfrak{A}$ satisfies all strict identities of the algebra $\mathfrak{P}_1 \times \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_k$ (direct product).

Def 2. Subdirectly representable in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ if $\mathfrak{A}$ is isomorphic with a suitable subdirect product of suitable subdirect powers of $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$.

Def 3. Semi-directly representable in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ if $\mathfrak{A}$ is isomorphic with the direct product of suitable subdirect powers of $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$.

Def 4. Directly representable in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ if $\mathfrak{A}$ is isomorphic with the direct product of suitable direct powers of $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$.

A portion of the fundamental structure theorem of [8] asserts[5])

Theorem 7. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ be an arbitrary independent class of primal algebras. Then the following four classes of algebras are pairwise coextensive up to isomorphisms:

(i) *The class of all $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$-algebras.*

(ii) *The class of all algebras subdirectly representable in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$.*

(iii) *The class of all algebras semi-directly representable in $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$.*

[5]) A second part asserts a certain *unicity* for the subdirect representation. The transformation of this unicity into primal-ideal form is not here considered.

(iv) *The class of all subalgebras of algebras directly representable in* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$.

Further, a finite $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ *- algebra is directly representable in* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$.

If in the proofs of theorems 4 and 5 we now appeal to theorem 7 rather than theorem 3, arguments parallel to those already given yield

Theorem 8. Let $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ *be a strictly independent class of primal algebras, and let* $\mathfrak{A}$ *be a* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$*-algebra. Then*

(i) *If* $\mathfrak{J}$ *is a primal ideal of* $\mathfrak{A}$, $\mathfrak{A}/\mathfrak{J} \cong \mathfrak{P}_i$, *where* $\mathfrak{P}_i$ *is a primal belonging to the class* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$.

(ii) *A primal ideal of* $\mathfrak{A}$ *is a maximal ideal, and conversely.*

(iii) *If* $\mathfrak{A} \neq \overset{\circ}{|}$ *then* $\mathfrak{A}$ *possesses at least one primal ideal.*

Theorem 9. Let $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ *be a strictly independent class of primal algebras, and let* $\mathfrak{A}$ *be a* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$*-algebra. Then each non-unit ideal of* $\mathfrak{A}$ *is the intersection of its maximal* (= *primal*) *ideal divisors.*

The applications of theorems 8, 9 are widespread. Thus for instance (see § 2),

from example (b): if $p_1, p_2, \ldots, p_k$ are distinct primes, the prime-fields $\{(F_{p_1}, \times, ^\circ), \ldots, (F_{p_k}, \times, ^\circ)\}$ form an independent primal class;

from example (c): if $n_1, n_2, \ldots, n_k$ are any distinct integers, with each $n_i > 1$, the corresponding n-fields $\{(\mathcal{F}_{n_1}, \times, ^\circ), \ldots, (\mathcal{F}_{n_k}, \times, ^\circ)\}$ form an independent primal class;

from example (e): if $n_1, n_2, \ldots, n_k$ are any distinct integers, with each $n_i > 1$, the corresponding basic Post-algebras $\{(P_{n_1}, \times, ^\circ), \ldots, (P_{n_k}, \times, ^\circ)\}$ form an independent primal class.

(For these and other strictly independent primal classes see [7].)

Bibliography

[1] Stone, M. H.: The theory of representations of Boolean algebras. Trans. Amer. Math. Soc. **40**, 37—111 (1936). — [2] McCoy, N. H., and Deane Montgomery: A representation of generalized Boolean rings. Duke Math. J. **3**, 455—459 (1937. — [3] McCoy, N. H.: Subdirect sums of rings. Bull. Amer. Math. Soc. **53**, 856—877 (1947). — [4] Rosenbloom, P.: The Elements of Mathematical Logic. The Dover Series (1950). — [5] Wade, L. I.: Post algebras and rings. Duke Math. J. **12**, 389—395 (1945). — [6] Birkhoff, G.: Subdirect unions in universal algebras. Bull. Amer. Math. Soc. **50**, 764—768(1944). — [7] Foster, A. L.: Generalized "Boolean" theory of universal algebras, Part I: Subdirect sums and normal representation theorem. Math. Z. **58**, 306—336 (1953), and Part II: Identities and subdirect sums of functionally complete algebras. Math. Z. **59**, 191—199 (1953). — [8] Foster, A. L.: The identities of—and unique subdirect factorization within—classes of universal algebras. Math. Z. **62**, 171—188 (1955). — [9] Foster, A. L.: The idempotent elements of a commutative ring form a Boolean algebra; ring duality and transformation theory. Duke Math. J. **12**, 143—152 (1945). — [10] Foster, A. L.: On n-ality theories in rings and their logical algebras, etc. Amer. J. Math. **72**, 101—123 (1950). — [11] Foster, A. L.: p-Rings and their Boolean-vector representation. Acta Math. Stockh. **84**, 231—261 (1950). — [12] Foster, A. L.: p-Rings and ring logics. Univ. California Publ. Math. **1**, 385—396 (1951). — [13] Yaqub, A.: On the theory of ring-logics and universal algebras. Doctoral dissertation, Univ. of California, Berkeley, (1955).

University of California, Berkeley

(Eingegangen am 24. Oktober 1955)

Krull, W.
Math. Zeitschr. Bd. 65, S. 76—90 (1956)

Über reelle Radikalkörper

Von
Wolfgang Krull

Die hier behandelten Probleme gehören zwar ihrer Natur nach in den Rahmen der „elementaren" bzw. „klassischen" Algebra, sie scheinen mir aber aus den folgenden Gründen bemerkenswert:

1. Während man mit Hilfe der Galoisschen Theorie die Radikalkörper schlechthin in allgemein bekannter Weise völlig befriedigend charakterisieren kann, findet sich über *reelle Radikalkörper* (in Zukunft kurz r. R.-Körper)[1] in der algebraischen Lehrbuchliteratur im allgemeinen nicht viel mehr als der folgende *p-Konjugiertensatz:* Ist der Grad des r. R.-Körpers $\mathfrak{K}$ über seinem Grundkörper $\mathfrak{K}_0$ eine Primzahl $p \neq 2$, so sind alle echten Konjugiertenkörper von $\mathfrak{K}$ über $\mathfrak{K}_0$ komplex[2]. Indessen ist es, wie in § 2 gezeigt wird, leicht möglich, die Klasse der r. R.-Körper von Primzahlgrad genau zu charakterisieren, und man stößt dabei auf zwei bemerkenswerte, meines Wissens bisher nicht beachtete Tatsachen[3]:

a) Die Gaußschen Primzahlen, also die von der Form $2^m + 1$, nehmen eine Sonderstellung ein. Nur bei ihnen liegen die Verhältnisse so einfach, wie man bei einer voreiligen Verallgemeinerung der bei den Körpern dritten Grades gemachten Erfahrungen allgemein erwarten könnte.

b) Will man bei einer nicht-Gaußschen Primzahl p eine hinreichende Kennzeichnung für die r. R.-Körper p-ten Grades erhalten, so muß man eine numerische Invariante heranziehen, die unter zahlentheoretischen Gesichtspunkten von Kummer bei der Entwicklung der Theorie der nach ihm benannten Körper eingeführt wurde. Das heißt aber, man muß in gewissem Sinne den

[1]) Unter einem reellen Radikalkörper (über dem Grundkörper $\mathfrak{K}_0$) verstehen wir einen Körper, der aus dem im üblichen Sinne reellen Körper $\mathfrak{K}_0$ durch Adjunktion einer reellen Radikalgröße entsteht, wobei die reelle Radikalgröße ihrerseits dadurch ausgezeichnet ist, daß zu ihrer Bildung außer den Elementen von $\mathfrak{K}_0$ nur *reelle* Nullstellen *reeller* binomischer Gleichungen benutzt werden. Vgl. im übrigen die exakten Definitionen am Anfang von § 1.

[2]) Ein echt konjugierter Körper von $\mathfrak{K}$ ist natürlich ein zu $\mathfrak{K}$ (über $\mathfrak{K}_0$) konjugierter Körper $\mathfrak{K}' \neq \mathfrak{K}$. Gewöhnlich erscheint der p-Konjugiertensatz in der Form: Ist eine Nullstelle α des über dem reellen Körper $\mathfrak{K}_0$ irreduziblen Polynoms $P(x)$ vom Primzahlgrade $p \neq 2$ eine reelle Radikalgröße, so sind alle anderen Nullstellen von $p(x)$ komplex. — Aber es zeigt sich bei weitergehenden Untersuchungen, daß man in der Theorie der r. R.-Körper zweckmäßig nur mit Körpern und ihren Isomorphismen und Automorphismen, nicht aber mit den erzeugenden Polynomen und definierenden Gleichungen der Körper arbeitet.

[3]) Den Inhalt von § 2 habe ich in den letzten 6 Jahren öfters in Vorlesungen und Seminaren behandelt, da sich hier eine ausgezeichnete Möglichkeit bietet, den Anfänger an einem historisch interessanten nichttrivialem Problem in die Anwendung der Galoisschen Theorie einzuführen.

Rahmen der klassischen Galoisschen Theorie überschreiten, — bei einem Problem, das letzten Endes vom „casus irreducibilis" der Gleichungen dritten Grades, also aus dem Gedankenkreis CARDANOs herstammt.

2. Es liegt äußerst nahe zu fragen: Gibt es eine sinnvolle Verallgemeinerung des fundamentalen p-Konjugiertensatzes auf reelle Radikalkörper beliebigen Grades[4])? Hier ist das wichtigste Ergebnis die Erkenntnis, daß nur durch eine ganz neue Begriffsbildung eine befriedigende Antwort gewonnen werden kann. Die Untersuchung beliebiger r.R.-Körper ist vor allem deshalb schwierig, weil diese Körper in der Regel *nicht* über ihrem Grundkörper $\mathfrak{K}_0$ normal sind. Um trotzdem vorwärts zu kommen, muß man beachten, daß jeder über $\mathfrak{K}_0$ normale Körper $\mathfrak{N}$ einen eindeutig bestimmten (mengentheoretisch), *maximalen* r.R.-Körper enthält. Beschränkt man sich auf maximale r.R.-Körper, so kommt man zu einfachen und in ihrer präzisen Form befriedigenden Sätzen, zu denen es, wie durch Beispiele gezeigt werden kann, bei beliebigen r.R.-Körpern kein Gegenstück gibt. Zunächst zeigt man leicht: Zu jedem maximalen r.R.-Körper $\mathfrak{K}$ existiert eine Körperkette

$$\mathfrak{K}_0 \subset \mathfrak{K}_1 \subset \cdots \subset \mathfrak{K}_m = \mathfrak{K},$$

bei der die Relativgrade $[\mathfrak{K}_i : \mathfrak{K}_{i-1}]$ sämtlich Primzahlen sind. Mit Hilfe dieses Satzes und der Theorie der r.R.-Körper vom Primzahlgrad gelingt dann weiter durch einen etwas mühsamen Induktionsschluß die gewünschte Verallgemeinerung des p-Konjugiertensatzes in der folgenden Form: Die zu einem maximalen r.R.-Körper echt konjugierten Körper sind alle komplex. — Die Anzahl der Automorphismen eines maximalen r.R.-Körpers ist stets eine Potenz von 2.

3. Die Erkenntnis von der Sonderstellung der maximalen r.R.-Körper zeigt einen Weg, auf dem vielleicht das — sicher schwierige — Problem der Charakterisierung aller r.R.-Körper ohne Gradbeschränkung erfolgreich angegriffen werden kann. Man wird voraussichtlich in erster Linie zu fragen haben: Welche Eigenschaften muß ein Normalkörper $\mathfrak{N}$ besitzen, wenn er der *kleinste* Normalkörper sein soll, der den in ihm steckenden maximalen r.R.-Körper umfaßt? — (In der vorliegenden Arbeit, in der der Konjugiertensatz für maximale r.R.-Körper das Hauptergebnis ist, gehen wir auf dieses Problem nicht näher ein.)

§1. Grundeigenschaften reeller Radikalkörper

Alle auftretenden Körper sollen in den Gaußschen Körper aller komplexen Zahlen eingebettet sein. Das Wort „reeller Körper" hat also den klassischen Sinn, nicht den formalen von ARTIN und VAN DER WAERDEN[5]). Wir stützen uns auf den folgenden wohlbekannten

[4]) Dabei ist nur an solche Sätze gedacht, die eine ähnlich scharfe Eindeutigkeitsaussage enthalten wie der Konjugiertensatz selbst.

[5]) Allerdings könnte man statt des Körpers aller gewöhnlichen reellen bzw. aller komplexen Zahlen einen beliebigen geordneten, reell abgeschlossenen Körper P bzw. den zugehörigen algebraisch abgeschlossenen Körper P^* wählen, ausschließlich Unter-

Hilfssatz 1. a) *Ist* $x^p - a$ $(a \in \mathfrak{K})$ *ein über dem Körper* $\mathfrak{K}$ *irreduzibles Binom, und wird* $x^p - a$ *über dem Körper* $\mathfrak{L} \supset \mathfrak{K}$ *reduzibel, so enthält* $\mathfrak{L}$ *mindestens eine Nullstelle von* $x^p - a$, *es zerfällt also speziell* $x^p - a$ *für* $p = 2$ *über* $\mathfrak{L}$ *in Linearfaktoren.* b) *Sind* $\mathfrak{K}$ *und* $\mathfrak{L}$ *reell, so enthält* $\mathfrak{L}$ *im Falle der Reduzibilität von* $x^p - a$ $(p \neq 2)$ *genau eine Nullstelle von* $x^p - a$, *nämlich die einzige reelle.*

Wir nennen $\mathfrak{K}$ einen *eigentlichen R-Körper* (Radikalkörper) über $\mathfrak{K}_0 < \mathfrak{K}$, wenn eine Körperkette $\mathfrak{K}_i = \mathfrak{K}_{i-1}(\alpha)$ $(i = 1, \ldots, m;\ \mathfrak{K}_m = \mathfrak{K})$ existiert, bei der α_i, jeweils Nullstelle eines über $\mathfrak{K}_{i-1}$ irreduzibeln Binoms $x^{p_i} - a_i$ $(a_i \in \mathfrak{K}_{i-1})$ vom Primzahlgrade p_i ist. Sind $\mathfrak{K}_0$ und alle α_i, also auch $\mathfrak{K}$, *reell*, so wird $\mathfrak{K}$ als *eigentlicher r.R.-Körper* (reeller Radikalkörper) über $\mathfrak{K}_0$ bezeichnet. Wo einer Untersuchungsreihe ein fester Ausgangskörper $\mathfrak{K}_0$ zugrunde liegt, wird „über $\mathfrak{K}_0$" weggelassen. Ein *R.-Körper* bzw. *r.R.-Körper* (über $\mathfrak{K}_0$) schlechthin ist jeder ($\mathfrak{K}_0$ enthaltende) Unterkörper eines eigentlichen R.-Körpers bzw. eigentlichen r.R.-Körpers. Jedes Element eines R.-Körpers bzw. r.R.-Körpers heißt *Radikalgröße* bzw. *reelle Radikalgröße* über $\mathfrak{K}_0$. Eine *erzeugende Radikalkette* des R.-Körpers $\mathfrak{K}$ über $\mathfrak{K}_0$ ist eine Kette von der Art, wie sie bei der Definition von $\mathfrak{K}$ benutzt wurde.

Satz 1. *a) Ist* $\mathfrak{K}$ *(eigentlicher) r.R.-Körper über* $\mathfrak{K}_0$, *so ist es* $\mathfrak{K}$ *auch über jedem Körper* $\mathfrak{K}_0'$ *zwischen* $\mathfrak{K}_0$ *und* $\mathfrak{K}$. *b) Der Vereinigungskörper* $\mathfrak{K} \cdot \mathfrak{L}$ *zweier (eigentlicher) r.R.-Körper über* $\mathfrak{K}_0$ *ist selbst ein (eigentlicher) r.R.-Körper über* $\mathfrak{K}_0$. *c) Ist* $\mathfrak{K}$ *ein (eigentlicher) r.R.-Körper über* $\mathfrak{K}_0$, $\mathfrak{L}$ *ein (eigentlicher) r.R.-Körper über* $\mathfrak{K}$, *so ist* $\mathfrak{L}$ *auch ein (eigentlicher) r.R.-Körper über* $\mathfrak{K}_0$.

a) und b) gelten ohne „eigentlich" trivialerweise, wenn sie mit „eigentlich" richtig sind. Um sie für eigentliche r.R.-Körper zu beweisen, sei $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_m$ eine erzeugende Radikalkette von $\mathfrak{K}$ bzw. $\mathfrak{L}$ über $\mathfrak{K}_0$. Dann folgt leicht aus Hilfssatz 1, vor allem 1b): a) Nach Weglassung aller der α_i bei denen $x^p - a_i$ über $\mathfrak{K}_0' \cdot \mathfrak{K}(\alpha_1, \ldots, \alpha_{i-1})$ reduzibel wird, wird die übrigbleibende Kette $\alpha_{i_1}, \ldots, \alpha_{i_r}$ eine erzeugende Radikalkette von $\mathfrak{K}$ über $\mathfrak{K}_0'$! b) Läßt man die β_k weg, für die $x^p - b_k$ über $\mathfrak{K} \cdot \mathfrak{K}_0(\beta_1, \ldots, \beta_{k-1})$ reduzibel ist, so stellt die mit den übrigbleibenden β gebildete Kette $\alpha_1, \ldots, \alpha_n, \beta_{k_1}, \ldots, \beta_{k_s}$ eine erzeugende Radikalkette von $\mathfrak{K} \cdot \mathfrak{L}$ über $\mathfrak{K}_0$ dar. c) Behauptung c) ist nach Definition bei *eigentlichen* r.R.-Körpern trivial. Im allgemeinen Fall gibt es sicher einen über $\mathfrak{K}_0$ bzw. $\mathfrak{K}$ eigentlichen r.R.-Körper $\mathfrak{K}^* \supseteq \mathfrak{K}$ bzw. $\mathfrak{L}^* \supseteq \mathfrak{L}$. Nach a) ist $\mathfrak{K}^*$ und nach b) auch $\mathfrak{K}^* \cdot \mathfrak{L}^*$ eigentlicher r.R.-Körper über $\mathfrak{K}$. Nach a) folgt weiter, daß $\mathfrak{K}^* \cdot \mathfrak{L}^*$ auch eigentlicher r.R.-Körper über $\mathfrak{K}^*$ sein muß, und da $\mathfrak{K}^*$ seinerseits eigentlicher r.R.-Körper über $\mathfrak{K}_0$, stellt $\mathfrak{K}^* \cdot \mathfrak{L}^* \supseteq \mathfrak{L}$ einen eigentlichen r.R.-Körper über $\mathfrak{K}_0$ dar.

körper von P^* betrachten und die Elemente von P auf Grund der gegebenen Ordnung als reell auszeichnen. Aber diese Verallgemeinerung ist offenbar uninteressant. Der entscheidende Punkt ist der, daß wir — zum mindesten dann, wenn unerträglich langwierige Konjugiertenbetrachtungen vermieden werden sollen — nicht allein von einem reellen, d.h. für uns geordneten, Grundkörper $\mathfrak{K}_0$ ausgehen können. Wir müssen auch von jedem auftretenden Oberkörper $\mathfrak{K}$ von $\mathfrak{K}_0$ von vornherein wissen, ob er reell (also in Fortsetzung der Ordnung von $\mathfrak{K}_0$ geordnet) ist oder nicht.

Um die Bedeutung von Satz 1 zu würdigen, beachte man: *Sind $\mathfrak{K}$ und $\mathfrak{L}$ eigentliche R-Körper über $\mathfrak{K}_0$, so braucht $\mathfrak{K} \cdot \mathfrak{L}$ kein eigentlicher R-Körper über $\mathfrak{K}_0$ zu sein.* Es sei etwa $\varepsilon = \exp \frac{2\pi i}{7}$ eine siebte Einheitswurzel, $\mathfrak{K}_0$ der Körper der rationalen Zahlen, α und $\alpha' = \varepsilon \cdot \alpha$ Nullstellen von $x^7 - 2$. Dann sind zwar $\mathfrak{K} = \mathfrak{K}_0(\alpha)$ und $\mathfrak{L} = \mathfrak{K}_0(\alpha')$, nicht aber $\mathfrak{K} \cdot \mathfrak{L} = \mathfrak{K}_0(\alpha, \alpha')$ eigentliche R-Körper über $\mathfrak{K}_0$. Denn wir haben $\mathfrak{K} \cdot \mathfrak{L} = \mathfrak{K}_0(\alpha, \varepsilon)$, es ist $\mathfrak{K} \cdot \mathfrak{L} = \mathfrak{N}$ über $\mathfrak{K}_0$ normal, und es gilt die Gradgleichung $[\mathfrak{N} : \mathfrak{K}_0] = 6$. Wäre also $\mathfrak{N}$ ein eigentlicher R-Körper über $\mathfrak{K}_0$, so müßte in einer erzeugenden Radikalkette $\alpha_1, \alpha_2, \alpha_3$ ein α_i auftreten, das über $\mathfrak{K}_0(\alpha_1, \ldots, \alpha_{i-1})$ Nullstelle eines Binoms $x^3 - a_i$ wäre. Wegen seiner Normalität müßte dann $\mathfrak{N}$ auch $\exp \frac{2\pi i}{3}$ enthalten, was nicht zutrifft. — Der Satz, daß $\mathfrak{K} \cdot \mathfrak{L}$ ein R-Körper über $\mathfrak{K}_0$ sein muß, wenn es $\mathfrak{K}$ und $\mathfrak{L}$ sind, ist zwar richtig, aber sein Beweis ist wesentlich umständlicher als der von Satz 1 b). Man muß, da Hilfssatz 1 b) nicht benutzt werden kann, zu mindesten einen neuen Hilfsbegriff einführen, nämlich den der „normierten Radikalketten“[6]). Aus Satz 1 b) folgt sofort: In jedem Körper $\mathfrak{M} \supset \mathfrak{K}_0$ gibt es einen größten r. R.-Körper $\mathfrak{K}$, nämlich den Vereinigungskörper aller der $\mathfrak{K}' \subseteq \mathfrak{M}$, die r. R.-Körper über $\mathfrak{K}_0$ sind[7]). Wir wollen nun $\mathfrak{K}$ als einen *maximalen r. R.-Körper über* $\mathfrak{K}_0$ bezeichnen, wenn $\mathfrak{K}$ der größte r. R.-Körper in dem zu $\mathfrak{K}$ über $\mathfrak{K}_0$ gehörigen Normalkörper $\mathfrak{N}$ (also in dem kleinsten, $\mathfrak{K}$ umfassenden über $\mathfrak{K}_0$ normalen Körper $\mathfrak{N}$) ist. Neben Satz 1 a) tritt dann ergänzend:

Satz 1 a′). Ist $\mathfrak{K}$ maximaler r. R.-Körper über $\mathfrak{K}_0$, so ist es $\mathfrak{K}$ auch über jedem Körper $\mathfrak{K}_0'$ zwischen $\mathfrak{K}_0$ und $\mathfrak{K}$.

Ist nämlich $\mathfrak{N}$ bzw. $\mathfrak{N}'$ der zu $\mathfrak{K}$ über $\mathfrak{K}_0$ bzw. $\mathfrak{K}_0'$ gehörige Normalkörper, so ist jedenfalls $\mathfrak{N}' \subseteq \mathfrak{N}$. Ist ferner $\mathfrak{L} \subseteq \mathfrak{N}'$ r. R.-Körper über $\mathfrak{K}_0'$, so ist es $\mathfrak{L}$ auch über $\mathfrak{K}_0$ [nach Satz 1 c)], und aus $\mathfrak{L} \subseteq \mathfrak{N}$ folgt $\mathfrak{L} \subseteq \mathfrak{K}$.

Satz 2. Ist $\mathfrak{K}$ ein maximaler r. R.-Körper über $\mathfrak{K}_0$, so gibt es stets eine Körperkette $\mathfrak{K}_0 \subset \mathfrak{K}_1 \subset \cdots \subset \mathfrak{K}_n = \mathfrak{K}$, bei der $[\mathfrak{K}_i : \mathfrak{K}_{i-1}] = p_i$ Primzahl $(i = 1, \ldots, n)$.

Wegen Satz 1a′) genügt es offenbar, zu zeigen: Es gibt einen Körper $\mathfrak{K}_1 \subseteq \mathfrak{K}$ bei dem $[\mathfrak{K}_1 : \mathfrak{K}_0] = p$ Primzahl. Es sei $\mathfrak{N}$ der zu $\mathfrak{K}$ über $\mathfrak{K}_0$ gehörige Normalkörper, $\mathfrak{K}^* \supseteq \mathfrak{K}$ ein eigentlicher r. R.-Körper über $\mathfrak{K}_0$. Ferner sei $\alpha_1, \ldots, \alpha_n$ eine erzeugende Radikalkette von $\mathfrak{K}^*$ über $\mathfrak{K}_0$, und es sei j so bestimmt, daß $\mathfrak{L} \cap \mathfrak{N} = \mathfrak{K}_0$, $\mathfrak{L}(\alpha_j) \cap \mathfrak{N} \supset \mathfrak{K}_0$ mit $\mathfrak{L} = \mathfrak{K}_0(\alpha_1, \ldots, \alpha_{j-1})$. Dann hat $\mathfrak{L}(\alpha_j) \cap \mathfrak{N} = \mathfrak{K}_1$ über $\mathfrak{K}_0$ den gleichen Primzahlgrad wie $\mathfrak{L}(\alpha_j)$ über $\mathfrak{L}$; ist etwa nämlich $\mathfrak{K}_1 = \mathfrak{K}_0(\beta)$ und $p(x)$ das über $\mathfrak{K}$ irreduzible Polynom mit der Nullstelle β, so muß $p(x)$ wegen der Normalität von $\mathfrak{N}$ und $\mathfrak{L} \cap \mathfrak{N} = \mathfrak{K}_0$ auch über $\mathfrak{L}$ irreduzibel

[6]) Zu den normierten Radikalketten vgl. etwa O. Haupt, Lehrbuch der Algebra, Band II (2. Aufl. 1953). Mit zu schwerem Geschütz schießen, hieße es, wenn man hier den Satz von der gruppentheoretischen Charakterisierung der normalen Radikalkörper heranziehen würde.

[7]) Wir beschränken uns stillschweigend auf endliche Erweiterungen des gegebenen Grundkörpers $\mathfrak{K}_0$, da auch der Begriff der r. R.-Körper nur für endliche Oberkörper von $\mathfrak{K}_0$ eingeführt wurde.

sein. $\mathfrak{K}_1$ ist als Unterkörper von $\mathfrak{K}^*$ ein r.R.-Körper über $\mathfrak{K}_0$ und aus der Maximalität von $\mathfrak{K}$ folgt $\mathfrak{K}_1 \subseteq \mathfrak{K}$.

Daß bei Satz 2 auf die Maximalität von $\mathfrak{K}$ über $\mathfrak{K}_0$ nicht verzichtet werden kann, zeigt das Beispiel eines Polynoms vierten Grades $p(x) = (x-\alpha_1) \cdot (x-\alpha_2) \cdot (x-\alpha_3) \cdot (x-\alpha_4)$ über dem Körper $\mathfrak{K}_0$ der rationalen Zahlen mit zwei reellen und zwei konjugiert komplexen Nullstellen α_1, α_2 bzw. α_3, α_4, dessen Gruppe die symmetrische ist. Hier hat die übliche kubische Resolvente eine reelle Nullstelle $\gamma_1 = (\alpha_1+\alpha_2-\alpha_3-\alpha_4)^2 = \beta_1^2$ $(\beta_1 > 0)$ und zwei konjugiert komplexe Nullstellen γ_2, γ_3. Nach CARDANO ist also $\mathfrak{K}_0(\gamma_1)$ ein r.R.-Körper über $\mathfrak{K}_0$, und das gleiche gilt für $\mathfrak{K}_0(\alpha_1, \alpha_2)$; denn $\mathfrak{K}_0(\gamma_1, \beta_1)$ bzw. $\mathfrak{K}_0(\alpha_1, \alpha_2)$ ist reell quadratisch über $\mathfrak{K}_0(\gamma_1)$ bzw. $\mathfrak{K}_0(\gamma_1, \beta_1)$. — Mit $\mathfrak{K}_0(\alpha_1, \alpha_2)$ ist auch $\mathfrak{K}_0(\alpha_1)$ ein r.R.-Körper über $\mathfrak{K}_0$. Aber man hat $[\mathfrak{K}_0(\alpha_1) : \mathfrak{K}_0] = 4$ und es läßt sich zwischen $\mathfrak{K}_0$ und $\mathfrak{K}_0(\alpha_1)$ kein echter Zwischenkörper einschieben.

Beachtet man, daß ein analoger Satz zu Satz 2 für jeden über $\mathfrak{K}_0$ normalen metazyklischen Körper gilt, während er für die Unterkörper von metazyklischen Normalkörpern nicht immer richtig ist, so erkennt man: *Die Maximalität ist bei den r.R.-Körpern ein gewisser Ersatz für die Normalität.* (Auf normale r.R.-Körper können wir uns nicht beschränken. Denn Hilfssatz 2 von § 2 zeigt, daß ein r.R.-Körper $\mathfrak{K}$ nur dann über $\mathfrak{K}_0$ normal sein kann, wenn $[\mathfrak{K} : \mathfrak{K}_0] = 2^m$.)

§2. Reelle Radikalkörper von Primzahlgrad

Hilfssatz 2. Ist $\mathfrak{K}$ r.R.-Körper über $\mathfrak{K}_0$ und $[\mathfrak{K} : \mathfrak{K}_0] = p \neq 2$ eine Primzahl, so sind alle echt Konjugierten von $\mathfrak{K}$ über $\mathfrak{K}_0$ komplex.

Hilfssatz 3. Ein reeller Abelscher Oberkörper des reellen Körpers $\mathfrak{K}_0$ von ungeradem Grad ist niemals r.R.-Körper über $\mathfrak{K}_0$.

Hilfssatz 2, der p-Konjugiertensatz der Einleitung, ist wohlbekannt. Hilfssatz 3 ist eine triviale Folgerung aus Hilfssatz 2. (Man beachte: Jeder Abelsche Oberkörper von $\mathfrak{K}_0$ enthält einen zyklischen Oberkörper mit $[\mathfrak{K} : \mathfrak{K}_0] = p$.) — Es sei jetzt $\mathfrak{K} = \mathfrak{K}_0(\alpha)$ ein fester Körper von ungeradem Primzahlgrad p über dem festen reellen Ausgangskörper $\mathfrak{K}_0$; $p(\alpha) = (x-\alpha_0) \dots (x-\alpha_{p-1})$. Sei das über $\mathfrak{K}_0$ irreduzible Polynom mit der reellen Nullstelle $\alpha = \alpha_0$, und es seien $\alpha_1, \dots, \alpha_{p-1}$ komplex. $\mathfrak{N} = \mathfrak{K}_0(\alpha_0, \dots, \alpha_{p-1})$ sei der zu $\mathfrak{K}$ über $\mathfrak{K}_0$ gehörige metazyklisch angenommene Normalkörper. Dann ist $\mathfrak{K}$ sicher nicht zyklisch über $\mathfrak{K}_0$. Nach der bekannten Theorie der metazyklischen Gleichungen von Primzahlgrad enthält $\mathfrak{N}$ einen über $\mathfrak{K}_0$ zyklischen Unterkörper $\mathfrak{Z}$, bei dem $t = [\mathfrak{Z} : \mathfrak{K}_0]$ ein Teiler von $p-1$, und für den $\mathfrak{N} = \mathfrak{Z} \cdot \mathfrak{K}_0(\alpha) = \mathfrak{Z} \cdot \mathfrak{K}_0(\alpha_i)$ $(i = 0, \dots, p-1;\ [\mathfrak{N} : \mathfrak{Z}] = p)$ gilt. Stellen wir die nicht-Abelsche Galoisgruppe $G(\mathfrak{N} : \mathfrak{K}_0)$ als Permutationsgruppe in den passend numerierten α_i dar, und setzen wir wie üblich $\alpha_k = \alpha_{k'}$, wenn $k \equiv k' (p)$, so besitzt $G(\mathfrak{N} : \mathfrak{K}_0)$ wie bekannt als Erzeugende die beiden Automorphismen $Z \equiv \{\alpha_i \to \alpha_{i+1}\}$ und $A \equiv \{\alpha_i \to \alpha_{s \cdot i}\}$; dabei ist s die kleinste positive Zahl mit den Eigenschaften $s^{t-1} \not\equiv 1 (p)$ und $s^t \equiv 1 (p)$. Der Invariantenkörper von Z bzw. A ist $\mathfrak{Z}$ bzw. $\mathfrak{K}_0(\alpha_0) = \mathfrak{K}$. Der durch A induzierte Automorphismus A_0 von $\mathfrak{Z}$ erzeugt die Gruppe $G(\mathfrak{Z} : \mathfrak{K}_0)$. Ist $[\mathfrak{Z} : \mathfrak{K}_0] = t = 2^m \cdot t_1$, $t_1 \equiv 2 (p)$, so besitzt $\mathfrak{Z}$ über $\mathfrak{K}_0$ eine direkte Zerlegung

$\mathfrak{Z} = \mathfrak{Z}_g \cdot \mathfrak{Z}_u$; $[\mathfrak{Z}_g : \mathfrak{K}_0] = 2^m$, $[\mathfrak{Z}_u : \mathfrak{K}_0] = t_1$. In entsprechender Weise läßt sich der über $\mathfrak{K}_0$ zyklische Körper $\mathfrak{K}_0(\varepsilon) = \mathfrak{E}\left(\varepsilon = \exp\frac{2\pi i}{p}\right)$ direkt zerlegen: $\mathfrak{E} = \mathfrak{E}_g \cdot \mathfrak{E}_u$; $[\mathfrak{E}_g : \mathfrak{K}_0] = 2^{m'}$, $[\mathfrak{E}_u : \mathfrak{K}_0] = t_1'$ $\left(t_1' \equiv 1(p),\ p - 1 \equiv 0(t_1')\right)$. Dabei sind $\mathfrak{Z}_u$ und $\mathfrak{E}_u$ reell; die Möglichkeiten $\mathfrak{Z}_u = \mathfrak{K}_0$, $\mathfrak{E}_u = \mathfrak{K}_0$ sind nicht ausgeschlossen, während sicher $\mathfrak{E}_g$ und $\mathfrak{Z}_g$ komplex, also von $\mathfrak{K}_0$ verschieden sind.

Satz 3. Ist $\mathfrak{K} = \mathfrak{K}_0(\alpha)$ ein r.R.-Körper über $\mathfrak{K}_0$, so gibt es einen reellen Quadratwurzelkörper $\mathfrak{K}_0'$ über $\mathfrak{K}_0$[8]*, derart daß $\mathfrak{N}' = \mathfrak{N} \cdot \mathfrak{K}_0' = \mathfrak{K}_0'(\varepsilon, \alpha)$; $[\mathfrak{N}' : \mathfrak{K}_0'] = 2pt_1$ $(t_1 \equiv 1(p))$.*

Den Beweis zerlegen wir in zwei Hauptabschnitte: a) *Es ist* $\mathfrak{Z}_u = \mathfrak{E}_u$. Es sei $\mathfrak{K}^*$ ein eigentlicher r.R.-Körper über $\mathfrak{K}_0$, der $\mathfrak{K}_0(\alpha)$ enthält; $\beta_1, \ldots, \beta_r$ sei eine erzeugende Radikalkette von $\mathfrak{K}^*$ und es sei $p(x)$ über $\mathfrak{L} = \mathfrak{K}(\beta_1, \ldots, \beta_{j-1})$ irreduzibel, über $\mathfrak{L}(\beta_j)$ reduzibel. Dann muß nach einer bekannten Verallgemeinerung von Hilfssatz 1 eine Nullstelle von $p(x)$ in $\mathfrak{L}(\beta_j)$ liegen[9], und das kann aus Realitätsgründen nur α sein. Weiter ergibt sich sofort: $\mathfrak{L}(\beta_j) = \mathfrak{L}(\alpha)$, $[\mathfrak{L}(\alpha) : \mathfrak{L}] = p$. Der zu $\mathfrak{L}(\alpha) = \mathfrak{L}(\beta_j)$ über $\mathfrak{L}$ gehörige Normalkörper $\mathfrak{N}_\mathfrak{L}$ ist einerseits gleich $\mathfrak{N} \cdot \mathfrak{L}$, andererseits gleich $\mathfrak{L}(\varepsilon)$. Daraus folgt $2^m \cdot t_1 \cdot p \equiv 0\ ([\mathfrak{N} \cdot \mathfrak{L} : \mathfrak{L}])$, $2^{m'} \cdot t_1' \cdot p \equiv 0\ ([\mathfrak{N} \cdot \mathfrak{L} : \mathfrak{L}])$. Für den über $\mathfrak{K}_0$ Abelschen, reellen Körper $\mathfrak{Z}_u \cdot \mathfrak{E}_u$ haben wir $t_1 \cdot t_1' \equiv 0\ ([\mathfrak{Z}_u \cdot \mathfrak{E}_u : \mathfrak{K}_0])$. Nach Hilfssatz 3 ergibt sich daraus $\mathfrak{L} \cap \mathfrak{Z}_u \cdot \mathfrak{E}_u = \mathfrak{K}_0$ und damit $[\mathfrak{N} \cdot \mathfrak{L} : \mathfrak{K}_0] \equiv 0\ ([\mathfrak{Z}_u \cdot \mathfrak{E}_u : \mathfrak{K}_0])$. Da nun $[\mathfrak{Z}_u \cdot \mathfrak{E}_u : \mathfrak{K}_0]$ durch das kleinste gemeinschaftliche Vielfache von t_1, t_1' teilbar und $t_1 \cdot t_1'$ zu $2p$ teilerfremd ist, sind die für $[\mathfrak{N} \cdot \mathfrak{L} : \mathfrak{L}]$ gefundenen Bedingungen nur dann miteinander verträglich, wenn $[\mathfrak{Z}_u : \mathfrak{K}_0] = [\mathfrak{E}_u : \mathfrak{K}_0] = [\mathfrak{Z}_u \cdot \mathfrak{E}_u : \mathfrak{K}_0]$ d.h. $\mathfrak{Z}_u = \mathfrak{E}_u$.

b) Es sei $\mathfrak{K}_0'$ größter reeller Unterkörper von $\mathfrak{Z}_g \cdot \mathfrak{E}_g$. Dann ist $[\mathfrak{Z}_g \cdot \mathfrak{E}_g : \mathfrak{K}_0'] = 2$ wegen der Normalität von $\mathfrak{K}_0'$ über dem reellen Körper $\mathfrak{K}_0$, und da $\mathfrak{K}_0'$ über $\mathfrak{K}_0$ Abelsch und reell, existiert für $\mathfrak{K}_0'$ über $\mathfrak{K}_0$ eine erzeugende Radikalkette $\varrho_1, \ldots, \varrho_m$, bei der $[\mathfrak{K}_0(\varrho_1, \ldots, \varrho_i) : \mathfrak{K}_0(\varrho_1, \ldots, \varrho_{i-1})] = 2$ $(i = 1, \ldots, m)$. Von den komplexen Körpern $\mathfrak{Z}_g$, $\mathfrak{E}_g$ ist keiner in $\mathfrak{K}_0'$ enthalten; es ist also $\mathfrak{Z}_g \cdot \mathfrak{K}_0' = \mathfrak{E}_g \cdot \mathfrak{K}_0' = \mathfrak{Z}_g \cdot \mathfrak{E}_g$. — Wir haben jetzt unter Berücksichtigung von $\mathfrak{E}_u = \mathfrak{Z}_u$: $\varepsilon \in \mathfrak{K}_0'(\alpha_0) \cdot \mathfrak{Z} = \mathfrak{K}_0' \cdot \mathfrak{N} = \mathfrak{N}'$, $\mathfrak{K}_0'(\varepsilon, \alpha) \subseteq \mathfrak{N}'$; $\mathfrak{Z} \subseteq \mathfrak{K}_0'(\varepsilon) = \mathfrak{K}_0' \cdot \mathfrak{E}$, $\mathfrak{N}' \subseteq \mathfrak{K}_0'(\varepsilon, \alpha)$, $\mathfrak{N}' = \mathfrak{K}_0(\varepsilon, \alpha)$. Schließlich ist $[\mathfrak{N}' : \mathfrak{K}_0'] = [\mathfrak{N}' : \mathfrak{K}_0'(\varepsilon)] \cdot [\mathfrak{K}_0'(\varepsilon) : \mathfrak{K}_0'] = p \cdot [\mathfrak{K}_0'(\varepsilon) : \mathfrak{K}_0']$; $[\mathfrak{K}_0'(\varepsilon) : \mathfrak{K}_0'] = [\mathfrak{K}_0'(\varepsilon) : \mathfrak{E}_u \cdot \mathfrak{K}_0'] \cdot [\mathfrak{E}_u \cdot \mathfrak{K}_0' : \mathfrak{K}_0'] = [\mathfrak{K}_0'(\varepsilon) : \mathfrak{E}_u \cdot \mathfrak{K}_0'] \cdot t_1$; $[\mathfrak{K}_0'(\varepsilon) : \mathfrak{E}_u \cdot \mathfrak{K}_0'] = [\mathfrak{K}_0' \cdot \mathfrak{E}_u \cdot \mathfrak{E}_g : \mathfrak{E}_u \cdot \mathfrak{K}_0'] = [\mathfrak{K}_0' \cdot \mathfrak{E}_g : \mathfrak{K}_0'] = [\mathfrak{Z}_g \cdot \mathfrak{E}_g : \mathfrak{K}_0'] = 2$, also $[\mathfrak{N}' : \mathfrak{K}_0'] = 2p\,t_1$.

[8]) Also ein reeller Oberkörper $\mathfrak{K}$ von $\mathfrak{K}_0$, zu dem eine Kette $\mathfrak{K}_0 < \mathfrak{K}_1 < \cdots < \mathfrak{K}_m = \mathfrak{K}$ mit $[\mathfrak{K}_i : \mathfrak{K}_{i-1}] = 2$ $(i = 1, \ldots, m)$ existiert, so daß jeweils $\mathfrak{K}_i = \mathfrak{K}_{i-1}(\sqrt{a_i})$ $(a_i \in \mathfrak{K}_{i-1},\ a_i > 0)$. Man beachte: a) Ein reeller Quadratwurzelkörper $\mathfrak{K}$ über $\mathfrak{K}_0$ ist stets ein r. Q.-Körper über $\mathfrak{K}_0$ mit $[\mathfrak{K} : \mathfrak{K}_0] = 2^m$; aber ein r.R.-Körper $\mathfrak{K}$ mit $[\mathfrak{K} : \mathfrak{K}_0] = 2^m$ braucht nicht immer ein reeller Quadratwurzelkörper über $\mathfrak{K}_0$ zu sein (vgl. das im Anschluß an Satz 2 von § 1 angegebene Beispiel). b) Ein maximaler r.R.-Körper $\mathfrak{K}$ mit $[\mathfrak{K} : \mathfrak{K}_0] = 2^m$ ist nach Satz 2 stets ein reeller Quadratwurzelkörper. c) Ein reeller Quadratwurzelkörper über $\mathfrak{K}_0$ kann auch charakterisiert werden, als ein reeller Unterkörper eines Normaloberkörpers $\mathfrak{N}$ von $\mathfrak{K}_0$, bei dem $[\mathfrak{N} : \mathfrak{K}_0] = 2^n$. (Unschwer einzusehen, wenn man beachtet, daß bei einem $\mathfrak{N}$ mit $[\mathfrak{N} : \mathfrak{K}_0] = 2^n$ wegen der Hyperauflösbarkeit der Gruppe zu jedem Unterkörper $\mathfrak{K}$ eine Kette $\mathfrak{K}_0 < \mathfrak{K}_1 < \cdots < \mathfrak{K}_m = \mathfrak{K}$ mit $[\mathfrak{K}_i : \mathfrak{K}_{i-1}] = 2$ existiert.)

[9]) Folgt aus der Tatsache, daß jede intransitive Untergruppe von $G(\mathfrak{N} : \mathfrak{K}_0)$ mindestens ein α_i fest lassen muß.

$\mathfrak{N}'$ baut sich über $\mathfrak{K}_0'$ nach dem gleichen Schema auf wie $\mathfrak{N}$ über $\mathfrak{K}_0$. Der wesentliche Unterschied ist nur der, daß an Stelle von $\mathfrak{Z}$ der Körper $\mathfrak{Z}' = \mathfrak{K}_0'(\varepsilon)$ tritt, und daß $[\mathfrak{Z}' : \mathfrak{K}_0'] = 2t_1$, statt $[\mathfrak{Z} : \mathfrak{K}_0] = 2^m \cdot t_1$ gilt. Wir betrachten nun unter Weglassung der ' und unter vorläufigem Verzicht auf die Gradbedingung allgemein den Fall, daß $\mathfrak{N} = \mathfrak{K}_0(\alpha) \cdot \mathfrak{Z} = \mathfrak{K}_0(\varepsilon, \alpha)$, $\mathfrak{Z} = \mathfrak{K}_0(\varepsilon)$ wird. Um hier eine notwendige und hinreichende Bedingung dafür zu erhalten, daß $\mathfrak{K}_0(\alpha)$ einen r. R.-Körper über $\mathfrak{K}_0$ darstellt, führen wir eine Zahlinvariante k von $\mathfrak{N}$ über $\mathfrak{K}_0$ ein, die aus historischen Gründen als die *Kummersche Invariante* bezeichnet werden kann[10]). Da $\mathfrak{N}$ über $\mathfrak{Z}$ zyklisch ist und ε in $\mathfrak{Z}$ liegt, gibt es für $\mathfrak{N}$ über $\mathfrak{Z}$ ein erzeugendes Binom $x^p - b$ $(b \in \mathfrak{Z})$, es wird also $\mathfrak{N} = \mathfrak{Z}(\beta)$, $\beta^p = b$. Bilden wir β^A mit dem oben eingeführten Automorphismus A, so muß wegen der Normalität von $\mathfrak{N}$ über $\mathfrak{K}_0$ auch $\mathfrak{N} = \mathfrak{Z}(\beta^A)$ werden, und daraus folgt eine leichte Rechnung $\beta^A = c \cdot \beta^k$ $(1 \leqq k \leqq p-1)$ in $\mathfrak{N}$, also $b^{A_0} = c^p \cdot \beta^k$ $(c \in \mathfrak{Z})$ in $\mathfrak{Z}$. Der Exponent k, von dem man mühelos zeigt, daß er nicht von der speziellen Wahl von b, sondern nur von $\mathfrak{N}$ und $\mathfrak{K}_0$ abhängt, ist die Kummersche Invariante von $\mathfrak{N} = \mathfrak{K}_0(\alpha, \varepsilon)$ über $\mathfrak{K}_0$. Aus der Definition von k folgt sofort:

Ist $\mathfrak{K}_0' > \mathfrak{K}_0$ und $\mathfrak{K}_0' \cap \mathfrak{N} = \mathfrak{K}_0$, so hat $\mathfrak{N}' = \mathfrak{K}_0' \cdot \mathfrak{N} = \mathfrak{K}_0'(\alpha, \varepsilon)$ über $\mathfrak{K}_0'$ dieselbe Kummersche Invariante k wie $\mathfrak{N}$ über $\mathfrak{K}_0$.

Man beachte: Wegen $\mathfrak{N} \cap \mathfrak{K}_0' = \mathfrak{K}_0$ sind die Gruppen $G(\mathfrak{N} : \mathfrak{K}_0)$ und $G(\mathfrak{N}' : \mathfrak{K}_0')$ isomorph und es ist die A zugeordnete Fortsetzung A' von A auf $\mathfrak{N}'$ für die Berechnung der Kummerschen Invariante k bei $\mathfrak{N}'$, $\mathfrak{K}_0'$ genau so brauchbar wie A bei $\mathfrak{N}$, $\mathfrak{K}_0$. Ist ferner $\mathfrak{N} = \mathfrak{Z}(\beta)$, $\beta^p = b \in \mathfrak{Z}$, so ist $\mathfrak{N}' = \mathfrak{Z}'(\beta')$ $(\mathfrak{Z}' = \mathfrak{Z} \cdot \mathfrak{K}_0')$ und aus $\beta = c \cdot \beta^A = c \cdot \beta^{A'}$, $c \in \mathfrak{Z} \subseteq \mathfrak{Z}'$ folgt sofort die Behauptung.

Satz 4. a) Hat $\mathfrak{N} = \mathfrak{K}_0(\alpha, \varepsilon)$ über $\mathfrak{K}_0$ die Kummersche Invariante $k = 1$, so ist $\mathfrak{K}_0(\alpha)$ eigentlicher r.R.-Körper über $\mathfrak{K}_0$. b) Ist $\mathfrak{N} = \mathfrak{K}_0(\alpha, \varepsilon)$, $[\mathfrak{N} : \mathfrak{K}_0] = 2p\,t_1$ $\left(t_1 \equiv 1(2)\right)$ und ist $\mathfrak{K}_0(\alpha)$ r.R.-Körper über $\mathfrak{K}_0$, so hat $\mathfrak{N}$ über $\mathfrak{K}_0$ die Kummersche Invariante 1.

Wir beginnen mit b). Ist $\mathfrak{K}_0(\alpha)$ r. R.-Körper über $\mathfrak{K}_0$, so gibt es nach einer schon beim Beweise von Satz 3 benutzten Überlegung einen r. R.-Körper $\mathfrak{K}_0'$ über $\mathfrak{K}_0$, derart, daß $[\mathfrak{K}_0'(\alpha) : \mathfrak{K}_0'] = p$ und gleichzeitig $\mathfrak{K}_0'(\alpha) = \mathfrak{K}_0'(\beta)$, wobei β Nullstelle eines über $\mathfrak{K}_0'$ irreduziblen Binoms $x^p - b$ $(b \in \mathfrak{K}_0')$. Aus $[\mathfrak{K}_0'(\alpha) : \mathfrak{K}_0] = p$, d. h. der Irreduzibilität von $p(x) = (x - \alpha_0) \cdot \cdots \cdot (x - \alpha_{p-1})$ über $\mathfrak{K}_0'$ folgt nach der bekannten Theorie der metazyklischen Gleichungen $\mathfrak{K}_0' \cap \mathfrak{N} = \mathfrak{K}_0' \cap \mathfrak{Z}$. Wegen $[\mathfrak{Z} : \mathfrak{K}_0] = [\mathfrak{Z}_g \cdot \mathfrak{Z}_u : \mathfrak{K}_0] = 2t_1$ muß aber $\mathfrak{K}_0' \cap \mathfrak{Z} = \mathfrak{K}_0$ sein; denn es ist ja $\mathfrak{K}_0' \cap \mathfrak{Z}_u = \mathfrak{K}_0$ nach Hilfssatz 3, und $\mathfrak{K}_0' \cap \mathfrak{Z}_g = \mathfrak{K}_0$, weil $\mathfrak{Z}_g$ ein komplexer Oberkörper zweiten Grades von $\mathfrak{K}_0$. Wegen $\mathfrak{K}_0' \cap \mathfrak{N} = \mathfrak{K}_0$ sind $G(\mathfrak{N} : \mathfrak{K}_0)$ und $G(\mathfrak{N} \cdot \mathfrak{K}_0' : \mathfrak{K}_0')$ isomorph und die Kummerschen Invarianten von $\mathfrak{N}$ über $\mathfrak{K}$ und $\mathfrak{N}'$ über $\mathfrak{K}_0'$ gleich. Die Kummersche Invariante von $\mathfrak{N}'$ über $\mathfrak{K}_0'$ schließlich ist offenbar gleich 1, da $b^{A'} = b$, $\beta^{A'} = \varepsilon^e \cdot \beta$, $\varepsilon^e \in \mathfrak{Z} \subseteq \mathfrak{Z} \cdot \mathfrak{K}_0'$.

Zum Beweise von a) genügt es, zu zeigen, daß ein reelles $\lambda \in \mathfrak{N}$ existiert, derart daß $\lambda^p = b \in \mathfrak{K}_0$ und $x^p - b$ irreduzibel über $\mathfrak{K}_0$. Denn dann muß

[10]) Zur Kummerschen Invariante vgl. etwa HILBERT, *Zahlbericht* (Gesammelte Abhandlungen I, 7.) § 125, Satz 147.

$p(x)=(x-\alpha_0)\cdot\ldots\cdot(x-\alpha_{p-1})$ über $\mathfrak{K}_0(\lambda)$ reduzibel werden; nach einer bereits bei Satz 3 benutzten Verallgemeinerung von Hilfssatz 1 muß also $\mathfrak{K}_0(\lambda)$ eine Nullstelle von $p(x)$ enthalten, und wegen der Realität von $\mathfrak{K}_0(\lambda)$ kann das nur $\alpha=\alpha_0$ sein[11]). — Wir bilden nun bei der zu Beginn des Paragraphen festgelegten Anordnung der α_i die Lagrangeschen Resolventen

$$(1)\qquad \lambda_q=\alpha_0+\sum_{k=1}^{p-1}\varepsilon^{q\cdot k}\cdot\alpha_k \qquad \left(\lambda_q=\lambda_{q'},\ \text{für}\ q\equiv q'(p)\right).$$

Ohne Beschränkung der Allgemeinheit dürfen wir $\lambda_1\neq 0$ annehmen[12]). Wegen $\mathfrak{Z}=\mathfrak{K}_0(\varepsilon)$ ist $\varepsilon^Z=\varepsilon$, $\varepsilon^{A_0}=\varepsilon^A=\varepsilon^{s'}$, wobei $s'^{t-1}=s'^{2t_1-1}\equiv 1(p)$, $s'^{t}=s'^{2t_1}\equiv 1(p)$, weil A_0 erzeugender Automorphismus von $G(\mathfrak{Z}:\mathfrak{K}_0)$. Mit $r\cdot s\equiv 1(p)$ ergibt sich:

$$(2)\qquad \lambda_1^A=\alpha_0+\sum_{k=1}^{p-1}\varepsilon^{s'\cdot k}\cdot\alpha_{s\cdot k}=\alpha_0+\sum_{k=1}^{p-1}\varepsilon^{s'\cdot r\cdot k}\cdot\alpha_k=\lambda_{s'\cdot r}.$$

(Man darf ja $s\cdot k$ durch k ersetzen, wenn man gleichzeitig $r\cdot k$ an Stelle von k schreibt.) Wegen $\lambda_q^Z=\varepsilon^{-q}$ und (2) haben wir: $(\lambda_1^A\cdot\lambda_1^{-k})^Z=\lambda_1^A\cdot\lambda_1^{-k}$, $\lambda_1^A\cdot\lambda_1^k\in\mathfrak{Z}$ für $k\equiv s'\cdot r(p)$, d.h.: Die Kummersche Invariante k von $\mathfrak{K}$ über $\mathfrak{K}_0$ ist charakterisiert durch $1\leq k\leq p-1$, $k\equiv s'\cdot r(p)$. Da nun $k=1$ nach Voraussetzung, muß $s'\cdot r\equiv 1(p)$, $\lambda_1^A=\lambda_1$ sein. Für $\lambda_1^p=b$ ergibt sich weiter: $b^A=b$, $b^Z=b$; $b\in\mathfrak{K}_0$. Weil schließlich $x^p-\lambda_1^p=x^p-b$ irreduzibel über $\mathfrak{K}_0$ ist und $\mathfrak{N}$ als Normalkörper über $\mathfrak{K}_0$ gleichzeitig mit λ_1 auch die reelle Nullstelle λ von x^p-b enthält, ist nach einer Bemerkung von weiter oben mit der Feststellung $b\in\mathfrak{K}_0$ der Beweis von Satz 4a) abgeschlossen. — Aus Satz 3 und Satz 4 zusammen ergibt sich unmittelbar:

I. Hauptsatz der r.R.-Körper von Primzahlgrad. Ein Oberkörper $\mathfrak{K}_0(\alpha)$ des reellen Körpers $\mathfrak{K}_0$ von ungeradem Primzahlgrad p ist dann und nur dann ein r.R.-Körper über $\mathfrak{K}_0$, wenn sich ein reeller Quadratwurzelkörper $\mathfrak{K}_0'$ über $\mathfrak{K}_0$ so bestimmen läßt, daß für den zu $\mathfrak{K}_0'(\alpha)$ über $\mathfrak{K}_0'$ gehörigen Normalkörper $\mathfrak{N}'$ die Gleichungen $\mathfrak{N}'=\mathfrak{K}_0'(\alpha,\varepsilon)$ $\left(\varepsilon=\exp\frac{2\pi i}{p}\right)$, $[\mathfrak{N}':\mathfrak{K}_0']=2p\,t_1$ $\left(t_1\equiv 1(2)\right)$ gelten, und wenn dabei außerdem $\mathfrak{N}'$ über $\mathfrak{K}_0'$ die Kummersche Invariante $k=1$ besitzt.

Sind nämlich die Voraussetzungen des Hauptsatzes erfüllt, so ist $\mathfrak{K}_0'(\alpha')$ nach Satz 4 r.R.-Körper über $\mathfrak{K}_0'$ und damit auch über $\mathfrak{K}_0$, da ja $\mathfrak{K}_0'$ seinerseits r.R.-Körper über $\mathfrak{K}_0$. Als Unterkörper von $\mathfrak{K}_0'(\alpha)$ ist also $\mathfrak{K}_0(\alpha)$ r.R.-Körper über $\mathfrak{K}_0$. — Ist andererseits $\mathfrak{K}_0(\alpha)$ r.R.-Körper über $\mathfrak{K}_0$, so existiert nach Satz 3 ein Quadratwurzelkörper $\mathfrak{K}_0'$ der im Hauptsatz geforderten Art und es ist $\mathfrak{K}_0'(\alpha)$ nach § 1 r.R.-Körper über $\mathfrak{K}_0'$. Nach Satz 4b) muß also $\mathfrak{N}'$ über $\mathfrak{K}_0'$ die Kummersche Invariante $k=1$ haben. — Am interessantesten ist beim ersten Hauptsatz die Feststellung, daß $\mathfrak{K}_0(\alpha)$ auch im Falle $\mathfrak{N}=\mathfrak{K}_0(\alpha,\varepsilon)$

[11]) Daß außer α_0 keine weitere Nullstelle reell sein kann, folgt ohne Zusatzvoraussetzung aus der Tatsache, daß $\mathfrak{N}$ komplex ist. Denn nach einem bekannten Satz wird $\mathfrak{N}=\mathfrak{K}_0(\alpha_0,\alpha_i)$, falls α_i beliebig aus der Reihe $\alpha_i,\ldots,\alpha_{p-1}$ gewählt.

[12]) Wir müssen dann allerdings unter Umständen für ε statt $\exp\left(\frac{2\pi i}{p}\right)$ eine andere primitive p-te Einheitswurzel wählen; doch ist das völlig nebensächlich.

keineswegs immer r.R.-Körper über $\mathfrak{K}_0$ zu sein braucht. (Man kann mit zahlentheoretischen Überlegungen leicht Beispiele konstruieren, in denen $\mathfrak{N} = \mathfrak{K}_0(\alpha, \varepsilon)$, $[\mathfrak{N}:\mathfrak{K}_0] = 2p\,t_1$, aber $k \neq 1$.) Einen wichtigen Sonderfall gibt es, in dem sich die Bedingungen von Hauptsatz 1 außerordentlich vereinfachen lassen. Es sei p eine *Gaußsche Primzahl*, also $p = 2^N + 1$. Dann wird $t_1 = t$, $\mathfrak{E}_u = \mathfrak{Z}_0 = \mathfrak{K}_0$, und es ist die Existenz des Quadratwurzelkörpers $\mathfrak{K}_0'$ nach dem Beweis von Satz 3 gesichert, sofern nur $\mathfrak{N} = \mathfrak{K}_0(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$ komplex. Weiter muß aber bei einer Gaußschen Primzahl die Kummersche Invariante k von $\mathfrak{N}'$ über $\mathfrak{K}_0'$ stets gleich 1 sein. Denn wir haben hier $s \not\equiv 1(p)$, $s' \not\equiv 1(p)$, $s^2 \equiv s'^2 \equiv 1(p)$, also $s \equiv s' \equiv -1(p)$, und aus $s \cdot r \equiv 1(p)$ folgt $s' \cdot r \equiv k \equiv 1(p)$. Für Gaußsche Primzahlen gilt also:

II. Hauptsatz der r.R.-Körper von Primzahlgrad. Ist $\mathfrak{K}_0(\alpha)$ reeller metazyklischer Oberkörper von $\mathfrak{K}_0$ und ist $[\mathfrak{K}_0(\alpha):\mathfrak{K}_0]$ eine Gaußsche Primzahl p, so ist $\mathfrak{K}_0(\alpha)$ dann und nur dann ein r.R.-Körper über $\mathfrak{K}_0$, wenn der zu $\mathfrak{K}_0(\alpha)$ über $\mathfrak{K}_0$ gehörige Normalkörper $\mathfrak{N}$ komplex ist.

(Zu unserer Formulierung der notwendigen Bedingung — im Vergleich zu Hilfssatz 3 — beachte man: Ist $\mathfrak{N}$ komplex, so müssen nach einem bekannten, auch weiter oben gelegentlich benutzten Satz[11]) *alle* echt Konjugierten von α komplex sein.) Hauptsatz II zeigt, daß 7 die kleinste Primzahl ist, bei der die eigentliche Problematik der r.R.-Körper von Primzahlgrad erkennbar wird.

§3. Beliebige maximale r.R.-Körper. Der Konjugiertensatz

Ein reeller Quadratwurzelkörper über $\mathfrak{K}_0$[8]) möge kurz als r.Q.-Körper über $\mathfrak{K}_0$ bezeichnet werden. Man beachte: Ist $\mathfrak{K}$ r.Q.-Körper über $\mathfrak{K}_0$, $\mathfrak{M}$ ein beliebiger reeller Oberkörper von $\mathfrak{K}_0$, so ist $\mathfrak{K}$ auch r.Q.-Körper über $\mathfrak{M}$.

Satz 5. Ist $\mathfrak{K}$ ein maximaler r.R.-Körper über $\mathfrak{K}_0$ mit dem zugehörigen Normalkörper $\mathfrak{N}$, und sind $p_1, \ldots, p_l$ die in $[\mathfrak{K}:\mathfrak{K}_0]$ aufgehenden ungeraden Primzahlen, so gibt es einen r.Q.-Körper $\mathfrak{K}^*$ über $\mathfrak{K}$, derart daß $\varepsilon_k \in \mathfrak{N} \cdot \mathfrak{K}^*$ $\left(\varepsilon_k = \exp\frac{2\pi i}{k};\ k = 1, \ldots, l\right)$.

Nach Satz 2 existieren für jede Primzahl p_k zwei Körper $\mathfrak{K}_{1k}$, $\mathfrak{K}_{2k}$, derart daß $\mathfrak{K}_0 \subseteq \mathfrak{K}_{1k} < \mathfrak{K}_{2k} \subseteq \mathfrak{K}$, $[\mathfrak{K}_{2k}:\mathfrak{K}_{1k}] = p_k$. Da dabei $\mathfrak{K}_{2k}$ r.R.-Körper über $\mathfrak{K}_{1k}$, gibt es nach Satz 3 einen r.Q.-Körper $\mathfrak{K}_k^*$ über $\mathfrak{K}_{1k}$, derart daß $\varepsilon_k \in \mathfrak{N}_k \cdot \mathfrak{K}_k^*$, falls $\mathfrak{N}_k$ der zu $\mathfrak{K}_{2k}$ über $\mathfrak{K}_{1k}$ gehörige, in $\mathfrak{N}$ enthaltene Normalkörper. Setzt man nun $\mathfrak{K}^* = \mathfrak{K}_1^* \cdot \ldots \cdot \mathfrak{K}_l^*$, so ist $\mathfrak{K}^*$ ein r.Q.-Körper über $\mathfrak{N}$ und $\varepsilon_k \in \mathfrak{N} \cdot \mathfrak{K}^*$ $(k = 1, \ldots, l)$.

Satz 6. Zu jedem maximalen r.R.-Körper $\mathfrak{K}$ über $\mathfrak{K}_0$ gibt es einen r.Q.-Körper $\mathfrak{K}^*$ über $\mathfrak{K}$, derart daß $\mathfrak{K}^*$ eigentlicher r.R.-Körper über $\mathfrak{K}_0$.

Für $[\mathfrak{K}:\mathfrak{K}_0] = 2$ ist die Behauptung trivial, für $[\mathfrak{K}:\mathfrak{K}_0] = p \neq 2$ (p Primzahl) folgt sie aus Satz 2 und Satz 3a) von § 2. [Man beachte: Ist $\mathfrak{K}_0'$ ein r.Q.-Körper über $\mathfrak{K}_0$, $\mathfrak{K}_0'(\alpha)$ eigentlicher r.R.-Körper über $\mathfrak{K}_0'$, so ist $\mathfrak{K}_0'(\alpha)$ eigentlicher r.R.-Körper über $\mathfrak{K}_0$ und r.Q.-Körper über $\mathfrak{K}_0'$.] — Im allgemeinen Fall gibt es nach Satz 2 jedenfalls einen Körper $\mathfrak{K}_1$, derart daß $[\mathfrak{K}_1:\mathfrak{K}_0]$ Primzahl (gerade oder ungerade). Wie bereits besprochen, existiert ein $\mathfrak{K}_1^*$, der r.Q.-Körper über $\mathfrak{K}_1$ und eigentlicher r.R.-Körper über $\mathfrak{K}_0$. Da ferner $\mathfrak{K}$ ein

maximaler r.R.-Körper über $\mathfrak{K}_1$ und da $[\mathfrak{K}:\mathfrak{K}_1]$ weniger Primfaktoren enthält als $[\mathfrak{K}:\mathfrak{K}_0]$, dürfen wir nach Induktionsprinzipien annehmen, daß es einen r.Q.-Körper $\mathfrak{K}_2^*$ über $\mathfrak{K}$ gibt, der eigentlicher r.R.-Körper über $\mathfrak{K}_1$ ist. $\mathfrak{K}_1^* \cdot \mathfrak{K}_2^* = \mathfrak{K}^*$ ist r.Q.-Körper über $\mathfrak{K}$, und die beim Beweise von Satz 1c) benutzten Überlegungen zeigen, daß $\mathfrak{K}^*$ ein eigentlicher r.R.-Körper über $\mathfrak{K}_0$ sein muß. - Daß bei Satz 5 und 6 die Beschränkung auf *maximale* r.R.-Körper wesentlich war, folgt aus der Bemerkung, daß das entscheidende Beweishilfsmittel der nur für maximale r.R.-Körper gültige Satz 2 war.

Satz 5 und Satz 6 legen den Gedanken nahe, es müßten sich wenigstens die maximalen r.R.-Körper ohne zusätzliche Einschränkung ebenso erschöpfend charakterisieren lassen wie die r.R.-Körper von Primzahlgrad. Indessen zeigt es sich rasch, daß dieses *Zentralproblem der r.R.-Körper* sicher keine einfache Aufgabe ist, und daß man jedenfalls nicht mit so primitiven Induktionsschlüssen zum Ziel kommt, wie bei Satz 5 und 6. Die Hauptschwierigkeit liegt darin, daß ein durch Übereinandertürmung relativer Normalkörper entstehender Körper nicht mehr über dem ursprünglichen Ausgangskörper normal zu sein braucht[13]). Wir müssen uns daher damit begnügen, wenigstens ein erstes, allgemeines Theorem zu beweisen:

Satz 7. Konjugiertensatz für maximale r.R.-Körper. Ist $\mathfrak{K}$ ein maximaler r.R.-Körper über $\mathfrak{K}_0$, so sind die zu $\mathfrak{K}$ über $\mathfrak{K}_0$ echt konjugierten Körper[2]) *alle komplex.*

Für $[\mathfrak{K}:\mathfrak{K}_0] = 2$ ist Satz 7 trivialerweise richtig; denn dann ist $\mathfrak{K}$ über $\mathfrak{K}_0$ normal und es gibt überhaupt keine echt konjugierten Körper zu $\mathfrak{K}$. Ist $[\mathfrak{K}:\mathfrak{K}_0]$ eine ungerade Primzahl p, so folgt die Richtigkeit von Satz 7 aus Hilfssatz 2. Im allgemeinen Fall sind wir am Ziel, wenn wir zeigen können: Gibt es einen echt konjugierten Körper zu $\mathfrak{K}$, so existiert stets ein über $\mathfrak{K}_0$ nicht normaler Körper $\mathfrak{K}_0'' \leqq \mathfrak{K}$ mit der Eigenschaft, daß alle zu $\mathfrak{K}_0''$ über $\mathfrak{K}_0$ echt konjugierten Körper komplex sind. Denn dann ist, falls $\mathfrak{N}$ der zu $\mathfrak{K}$ über $\mathfrak{K}_0$ gehörige Normalkörper, der Normalisator von $G(\mathfrak{N}:\mathfrak{K}_0'')$ wegen der Nichtnormalität von $\mathfrak{K}_0''$ eine echte Untergruppe von $G(\mathfrak{N}:\mathfrak{K}_0)$, es ist also der Invariantenkörper $\mathfrak{K}_0'$ dieses Normalisators ein echter Oberkörper von $\mathfrak{K}_0$. Ferner ist klar, daß in unserem Falle alle zu $\mathfrak{K}$ über $\mathfrak{K}_0$ echt konjugierten Körper komplex sind, wenn nur die zu $\mathfrak{K}$ über $\mathfrak{K}_0'$ echt konjugierten Körper diese Eigenschaft haben. Das aber dürfen wir nach Induktionsprinzip als gesichert annehmen, da $\mathfrak{K}$ auch ein maximaler r.R.-Körper über $\mathfrak{K}_0'$ und $[\mathfrak{K}:\mathfrak{K}_0']$ ein echter Teiler von $[\mathfrak{K}:\mathfrak{K}_0]$. — Bei der Konstruktion von $\mathfrak{K}_0''$ unterscheiden wir mehrere Fälle:

a) Es sei $\mathfrak{K}$ ein Quadratwurzelkörper über $\mathfrak{K}_0$, also $[\mathfrak{K}:\mathfrak{K}_0] = 2^g$ und es sei $\mathfrak{N}_0$ der größte in $\mathfrak{K}$ enthaltene, über $\mathfrak{K}_0$ normale Körper. Für $\mathfrak{N}_0 = \mathfrak{K} = \mathfrak{N}$ ist Satz 7 trivial richtig. Sei also $\mathfrak{N}_0 < \mathfrak{K}$; da $\mathfrak{K}$ ein maximaler r.R.-Körper

[13]) Daß man möglicherweise diese Schwierigkeit dadurch umgehen kann, daß man von den maximalen r.R.-Körpern zu den zugehörigen Normalkörpern übergeht, wurde am Schluß der Einleitung angedeutet. Allerdings dürfte auch die Charakterisierung dieser Normalkörper keineswegs einfach sein. Am besten beginnt man vielleicht mit der Betrachtung von Spezialfällen, etwa mit dem Studium der komplizierteren Normalkörper, die unter e) bei dem Induktionsbeweis von Satz 7 auftreten.

über $\mathfrak{K}_0$, existiert ein Körper $\mathfrak{K}_1$ mit $\mathfrak{N}_0 < \mathfrak{K}_1 \leqq \mathfrak{K}$; $[\mathfrak{K}_1 : \mathfrak{N}_0] = 2$. Der zu $\mathfrak{K}_1$ über $\mathfrak{K}_0$ gehörige Normalkörper $\mathfrak{N}_1$ ist das Produkt von endlich vielen über $\mathfrak{N}_0$ quadratischen Körpern $\mathfrak{K}_1 = \mathfrak{K}', \mathfrak{K}'', \ldots$ und es ist $\mathfrak{N}_1$ sicher komplex, weil $\mathfrak{N}_1$ im Falle der Realität wegen der Maximaleigenschaft von $\mathfrak{K}$ in $\mathfrak{K}$ enthalten sein müßte, was der Definition von $\mathfrak{N}_0$ widerspricht. Es seien nun etwa $\mathfrak{K}_1 = \mathfrak{K}', \ldots, \mathfrak{K}^{(\varrho)}$ reell, $\mathfrak{K}^{(\varrho+1)}, \mathfrak{K}^{(\varrho+2)}, \ldots$ komplex, $\mathfrak{K}_0'' = \mathfrak{K}' \cdot \mathfrak{K}'' \cdot \ldots \cdot \mathfrak{K}^{(\varrho)}$. Da jeder Automorphismus A_1 von $\mathfrak{N}_1$ über $\mathfrak{K}_0$ einen Automorphismus A_0 von $\mathfrak{N}_0$ induziert, vertauschen sich bei jedem A_1 die Körper $\mathfrak{K}', \mathfrak{K}'', \ldots$ untereinander und man hat zwei Möglichkeiten: Entweder es geht bei A_1 jedes $\mathfrak{K}^{(\nu)}$ $(\nu \leqq \varrho)$ wieder in ein $\mathfrak{K}^{(\mu)}$ $(\mu \leqq \varrho)$ über; dann induziert A_1 einen Automorphismus von $\mathfrak{K}_0''$. Oder es hat für mindestens ein $\nu \leqq \varrho$ das Bild von $\mathfrak{K}^{(\nu)}$ relativ A_1 einen Index $\mu > \varrho$; dann bilden A_1 den Körper $\mathfrak{K}_0''$ auf einen komplexen Körper ab. Die echt Konjugierten von $\mathfrak{K}_0''$ über $\mathfrak{K}_0$ sind also alle komplex. Außerdem ist $\mathfrak{K}_0''$ als Produkt von r. Q.-Körpern selbst ein r. Q.-Körper über $\mathfrak{N}_0$ und damit auch ein r. R.-Körper über $\mathfrak{K}_0$.

b) Offenbar gibt es in $\mathfrak{K}$ einen größten r. Q.-Körper $\mathfrak{K}_q$, den Vereinigungskörper aller der $\mathfrak{L} \leqq \mathfrak{K}$, die über $\mathfrak{K}_0$ r. Q.-Körper sind. Ist $\mathfrak{K}_q = \mathfrak{K}_0$, so enthält $\mathfrak{K}$ einen Körper $\mathfrak{K}_1$, dessen Grad über $\mathfrak{K}_0$ eine ungerade Primzahl p ist. Hilfssatz 2 von § 2 zeigt, daß $\mathfrak{K}_1$ über $\mathfrak{K}_0$ nicht normal sein kann, und daß alle echt konjugierten Körper von $\mathfrak{K}_1$ komplex sind. Wir können also $\mathfrak{K}_0'' = \mathfrak{K}_1$ setzen und sind am Ziel.

c) Es sei $\mathfrak{K}_q > \mathfrak{K}_0$, aber von dem zugehörigen Normalkörper $\mathfrak{N}_q$ (über $\mathfrak{K}_0$) verschieden. Dann ist, wie sofort zu sehen, der Grad $[\mathfrak{N}_q : \mathfrak{K}_0]$ eine Potenz von 2. Der größte in $\mathfrak{N}_q$ enthaltene r. R.-Körper $\mathfrak{K}_q'$ ist also ein r. Q.-Körper über $\mathfrak{K}_0$. Aus der Maximalität von $\mathfrak{K}_q'$ folgt $\mathfrak{K}_q' \geqq \mathfrak{K}_q$ und aus der Maximalität von $\mathfrak{K}$ sowie $\mathfrak{K}_q$ ergibt sich $\mathfrak{K}_q' \leqq \mathfrak{K}$, $\mathfrak{K}_q' \leqq \mathfrak{K}_q$. Es ist also $\mathfrak{K}_q$ ein maximaler, nicht-normaler r. R.-Körper über $\mathfrak{K}_0$ und die Überlegungen von a) zeigen, daß bereits in $\mathfrak{K}_q$ ein Körper $\mathfrak{K}_0''$ der gewünschten Art enthalten ist.

d) Es sei jetzt $\mathfrak{K}_q = \mathfrak{N}_q$ über $\mathfrak{K}_0$ normal und $\mathfrak{K}_0 < \mathfrak{N}_q < \mathfrak{K}$. Nach Satz 2 gibt es in $\mathfrak{K}$ einen Körper $\mathfrak{K}_{q_1} > \mathfrak{N}_q$, bei dem $[\mathfrak{K}_{q_1} : \mathfrak{N}_q] = p$ eine ungerade Primzahl. Ist der zu $\mathfrak{K}_{q_1}$ über $\mathfrak{N}_q$ gehörige Normalkörper $\mathfrak{N}_{q_1}$ auch über $\mathfrak{K}_0$ normal, so ist $\mathfrak{K}_{q_1} = \mathfrak{K}_0''$ ein Körper des gesuchten Typs. Denn $\mathfrak{K}_{q_1}$ ist als r. R.-Körper vom Relativgrad p nicht einmal über $\mathfrak{N}_q$ normal, und es muß jeder zu $\mathfrak{K}_{q_1}$ über $\mathfrak{K}_0$ konjugierte Körper ein in $\mathfrak{N}_{q_1}$ enthaltener Oberkörper von $\mathfrak{N}_q$ vom Relativgrad p über $\mathfrak{N}_q$ sein. Die einzigen derartigen Körper sind aber die Konjugierten von $\mathfrak{K}_{q_1}$ über $\mathfrak{N}_q$, und daß unter diesen $\mathfrak{K}_{q_1}$ selbst der einzige reelle Körper ist, zeigt Hilfssatz 2. — Es bleibt also nur noch ein letzter schwierigster Fall übrig, nämlich: $\mathfrak{K}_0 < \mathfrak{K}_q = \mathfrak{N}_q < \mathfrak{K}$; zu dem Normalkörper $\mathfrak{N}_{q_1}$ der zu dem Körper $\mathfrak{K}_{q_1}$ über $\mathfrak{N}_q$ gehört, gibt es über $\mathfrak{K}_0$ mehrere konjugierte Körper $\mathfrak{N}_{q_1}, \mathfrak{N}_{q_2}, \ldots, \mathfrak{N}_{q_l}$. Hier erfordert die Konstruktion von $\mathfrak{K}_0''$ mehrere Schritte.

e) α) Nach § 2 enthält $\mathfrak{N}_{qi}$ einen über $\mathfrak{N}_q$ zyklischen Körper $\mathfrak{Z}_i$; wie in § 2 zerlegen wir $\mathfrak{Z}_i$ in zwei Faktoren: $\mathfrak{Z}_i = \mathfrak{Z}_{gi} \cdot \mathfrak{Z}_{qi}$ $[\mathfrak{Z}_{gi} : \mathfrak{N}_q] = 2^\varrho$, $[\mathfrak{Z}_{ui} : \mathfrak{N}_q] \not\equiv 0 \,(2)$ $(i = 1, \ldots, l)$. Natürlich sind die $\mathfrak{Z}_{gi}$ und ebenso die $\mathfrak{Z}_{ui}$ über $\mathfrak{K}_0$ konjugiert. Da $\mathfrak{K}_{q1}$ ein r. R.-Körper über $\mathfrak{N}_q$, ist $\mathfrak{Z}_{u1}$ nach Satz 3 der Vereinigungskörper

von $\mathfrak{R}_q$ und dem größten Unterkörper von $\mathfrak{K}_0(\varepsilon)$, der über $\mathfrak{K}_0$ ungeraden Grad besitzt. Das heißt aber: $\mathfrak{Z}_{u1}$ ist als Produkt zweier über $\mathfrak{K}_0$ normaler Körper selbst über $\mathfrak{K}_0$ normal, und wir haben daher: $\mathfrak{Z}_{u1} = \mathfrak{Z}_{u2} = \cdots = \mathfrak{Z}_{ul} = \mathfrak{Z}_u$. Weiter zeigen wir: Es ist auch $\mathfrak{Z}_{g1} = \mathfrak{Z}_{g2} = \cdots = \mathfrak{Z}_{gl} = \mathfrak{Z}_g$ und überdies $[\mathfrak{Z}_g : \mathfrak{R}_q] = 2$. Es ist nämlich jedenfalls $\mathfrak{Z}_{g1} \cdot \mathfrak{Z}_{g2} \cdot \cdots \cdot \mathfrak{Z}_{gl} = \mathfrak{A}$ über $\mathfrak{R}_q$ Abelsch und $[\mathfrak{A} : \mathfrak{R}_q] = 2^\varrho$ $(\varrho \geqq 1)$. Wäre nun $\varrho > 1$, so wäre nach einer im wesentlichen schon in § 2 benützten Überlegung der größte reelle Unterkörper $\mathfrak{A}'$ von $\mathfrak{A}$ vom Grade $2^{\varrho-1} > 1$ über $\mathfrak{R}_q$ und außerdem ein r. Q.-Körper über $\mathfrak{R}_q$. Das aber widerspricht der Maximaleigenschaft von $\mathfrak{R}_q$. Wir haben also: $[\mathfrak{A} : \mathfrak{R}_q] = 2$ und das ist gerade die zu beweisende Behauptung.

β) Nach e, α) enthalten die über $\mathfrak{R}_q$ normalen Körper $\mathfrak{R}_{qi}$ alle ein und denselben größten über $\mathfrak{R}_q$ zyklischen Unterkörper $\mathfrak{Z} = \mathfrak{Z}_g \cdot \mathfrak{Z}_q$ und aus dem Beweis von Satz 3 in § 2 folgt: Es gibt einen r. Q.-Körper $\mathfrak{R}'_q$ über $\mathfrak{R}_q$, derart daß $\mathfrak{R}'_{qi} = \mathfrak{R}'_q \cdot \mathfrak{R}_{qi} = \mathfrak{R}'_q(\varepsilon, \alpha^{(i)})$ $\left(\varepsilon = \exp\left(\frac{2\pi i}{p}\right)\right)$, falls $\alpha^{(i)}$ jeweils in $\mathfrak{R}_{qi}$ so gewählt, daß $[\mathfrak{R}_q(\alpha^{(i)}) : \mathfrak{R}_q] = p$. (Man beachte, daß die Existenz des kritischen r. Q.-Körpers bei Satz 3 allein auf Grund der speziellen Struktur von $\mathfrak{Z}$ bewiesen wurde.) Wir zeigen nun: $\mathfrak{R}'_q$ *ist normal über* $\mathfrak{K}_0$. — Es sei wie in § 2 $\mathfrak{E}_g$ der größte Unterkörper von $\mathfrak{K}_0(\varepsilon)$ mit $[\mathfrak{E}_g : \mathfrak{K}_0] = 2^m$; $\mathfrak{E}'_g$ sei der größte reelle Unterkörper von $\mathfrak{E}_g$. Dann ist jedenfalls $\mathfrak{R}''_q = \mathfrak{E}'_g \cdot \mathfrak{R}_q$ als Produkt zweier über $\mathfrak{K}_0$ normaler Unterkörper selbst über $\mathfrak{K}_0$ normal und es ist $\mathfrak{R}_{q'}$ nach dem Beweis von Satz 3 der größte reelle Unterkörper von $\mathfrak{Z}_g \cdot \mathfrak{E}_g$, woraus wegen $[\mathfrak{E}_g : \mathfrak{E}'_g] = [\mathfrak{Z}_g : \mathfrak{R}_q] = 2$ sofort zu schließen, daß entweder $[\mathfrak{Z}_g \cdot \mathfrak{E}_g : \mathfrak{R}''_q] = 2$, $\mathfrak{R}''_q = \mathfrak{R}'_q$ oder $[\mathfrak{Z}_g \cdot \mathfrak{E}_g : \mathfrak{R}''_q] = 4$, $[\mathfrak{R}'_q \cdot \mathfrak{R}''_q] = 2$. Im ersten Fall sind wir fertig. Im zweiten kann man so schließen. Es enthält $\mathfrak{Z}_g \cdot \mathfrak{E}_g$ drei über $\mathfrak{R}''_q$ quadratische Körper. Von ihnen sind zwei nämlich $\mathfrak{Z}_g \cdot \mathfrak{E}'_g$ und $\mathfrak{E}_g \cdot \mathfrak{R}''_q$, Produkte über $\mathfrak{K}_0$ normaler Körper und damit selbst normal; also muß auch $\mathfrak{R}'_q$, der dritte, über $\mathfrak{K}_0$ normal sein.

γ) Da $\mathfrak{K}_{q1}$ r. R.-Körper über $\mathfrak{K}_0$ und über $\mathfrak{R}_q$, existiert nach § 2 ein Binom $x^p - b_1$ $(b_1 \in \mathfrak{R}'_q)$ mit der reellen Nullstelle β_1, derart daß $\mathfrak{K}_{q1} \subseteqq \mathfrak{R}'_q(\beta_1)$ und es gibt dann für *jede* Nullstelle β'_1 von $x^p - b_1$ in $\mathfrak{R}'_q(\beta'_1)$ einen Unterkörper von $\mathfrak{R}_{q1}$ vom Grade p über $\mathfrak{R}_q$. Es sei jetzt A_i ein Isomorphismus über $\mathfrak{K}_0$ von $\mathfrak{R}_{q1}$ auf $\mathfrak{R}_{qi}$, A'_i sei eine Fortsetzung von A_i, die $\mathfrak{R}'_{q1} = \mathfrak{R}'_q \cdot \mathfrak{R}_{q1}$ in $\mathfrak{R}'_{qi} = \mathfrak{R}'_q \cdot \mathfrak{R}_{qi}$ überführt. Bei A_i geht $x^p - b_1$ in ein Binom $x^p - b_i$ $(b_i \in \mathfrak{R}'_q)$ über und aus Isomorphiegründen muß für jede Nullstelle β_i von $x^p - b_i$ in $\mathfrak{R}'_q(\beta_i)$ ein Unterkörper $\mathfrak{K}_{qi}$ von $\mathfrak{R}_{qi}$ enthalten sein. Wählen wir für β_i speziell die reelle Nullstelle von $x^p - b_i$, so erweist sich $\mathfrak{K}_{qi}$ als r. R.-Körper über $\mathfrak{R}'_q$ und damit auch über $\mathfrak{K}_0$. Damit ist nach Hilfssatz 2 gleichzeitig gezeigt: Alle zu $\mathfrak{K}_{qi}$ über $\mathfrak{R}_q$ echt konjugierten Körper (und das sind alle von $\mathfrak{K}_{qi}$ verschiedenen Unterkörper von $\mathfrak{R}_{qi}$, die über $\mathfrak{R}_q$ den Grad p haben), sind komplex. Aus der letzten Bemerkung folgt sofort, die sämtlichen zu dem Körper $\mathfrak{K}''_0 = \mathfrak{K}_{q1} \cdot \cdots \cdot \mathfrak{K}_{ql}$ über $\mathfrak{K}_0$ echt konjugierten Körper sind komplex. Denn bei jedem Automorphismus A des zu $\mathfrak{K}''_0$ über $\mathfrak{K}_0$ gehörigen Normalkörpers $\mathfrak{R}_{q1} \cdot \cdots \cdot \mathfrak{R}_{ql}$ vertauschen sich die $\mathfrak{R}_{qi}$ nur untereinander, und da $\mathfrak{R}_q$ über $\mathfrak{K}_0$ normal, muß bei A jeder der Körper $\mathfrak{K}_{qi}$ in einen Körper übergehen, der in

einem $\mathfrak{N}_{q\,k}$ enthalten ist und über $\mathfrak{N}_q$ den Grad p besitzt. Im übrigen ist $\mathfrak{K}_0''$ nicht normal und ein r.R.-Körper über $\mathfrak{K}_0$, also in dem maximalen r.R.-Körper $\mathfrak{K}$ enthalten. Wir haben also auch im schwierigsten Fall die Konstruktion von $\mathfrak{K}_0'$ durchgeführt und damit den Beweis des Konjugiertensatzes abgeschlossen.

§4. Der Automorphismensatz. Ergänzungsbemerkungen

Der Konjugiertensatz für maximale r.R.-Körper wird ergänzt durch den Automorphismensatz:

Satz 8. Die Anzahl σ der Automorphismen eines maximalen r.R.-Körpers $\mathfrak{K}$ über seinem Grundkörper $\mathfrak{K}_0$ ist stets eine Potenz von 2: $\sigma = 2^m$ $(0 \leq m)$[14]).

Es sei $\mathfrak{N}$ der zu $\mathfrak{K}$ über $\mathfrak{K}_0$ gehörige Normalkörper und es werde für $\mathfrak{N} \geqq \mathfrak{L} \geqq \mathfrak{K}_0$ kurz $G_\mathfrak{L} = G(\mathfrak{N}:\mathfrak{L})$ gesetzt; $N_\mathfrak{L}(G_\mathfrak{K})$ sei der Normalisator von $G_\mathfrak{K}$ in $G_\mathfrak{L}$ $(\mathfrak{K} \geqq \mathfrak{L} \geqq \mathfrak{K}_0)$. Die zu bestimmende Automorphismenzahl ist dann gleich dem Index $[N_{\mathfrak{K}_0}(G_\mathfrak{K}):G_\mathfrak{K}]$ von $G_\mathfrak{K}$ in $N_{\mathfrak{K}_0}(G_\mathfrak{K})$. — Für $\mathfrak{K} = \mathfrak{K}_0$ wird $G_\mathfrak{K} = N_{\mathfrak{K}_0}(G_\mathfrak{K}) = G_{\mathfrak{K}_0}$, $\sigma = 1 = 2^0$. Wir dürfen also die Induktionsvoraussetzung machen, daß für $\mathfrak{K} \geqq \mathfrak{K}_1 > \mathfrak{K}_0$ bereits $[N_{\mathfrak{K}_1}(G_\mathfrak{K}):G_\mathfrak{K}] = 2^{m_1}$ bewiesen sei. Es sei dabei $\mathfrak{K}_1$ nach Satz 2 insbesondere so gewählt, daß $[\mathfrak{K}_1:\mathfrak{K}_0]$ Primzahl. Dann unterscheiden wir zwei Fälle:

a) $[\mathfrak{K}_1:\mathfrak{K}_0] = p \neq 2$. Hier besitzt der Körper $\mathfrak{K}_1$, der ja nach Hilfssatz 2 nicht über $\mathfrak{K}_0$ normal ist, nur den identischen Automorphismus, und es wird daher $N_{\mathfrak{K}_0}(G_\mathfrak{K}) = N_{\mathfrak{K}_1}(G_\mathfrak{K})$, $\sigma = [N_{\mathfrak{K}_1}(G_\mathfrak{K}):G_\mathfrak{K}] = 2^{m_1}$.

b) $[\mathfrak{K}_1:\mathfrak{K}_0] = 2$. Hier gibt es einen einzigen echten Automorphismus A_1 von $\mathfrak{K}_1$ über $\mathfrak{K}_0$. Wir haben daher $[N_{\mathfrak{K}_0}(G_\mathfrak{K}):N_{\mathfrak{K}_1}(G_\mathfrak{K})] = 2$ bzw. $= 1$, je nachdem ob sich A_1 zu einem Automorphismus A von $\mathfrak{K}$ über $\mathfrak{K}_0$ fortsetzen läßt oder nicht. Mit der Voraussetzung $[N_{\mathfrak{K}_1}(G_\mathfrak{K}):G_\mathfrak{K}] = 2^{m_1}$ erhalten wir somit für σ die beiden Möglichkeiten $\sigma = 2^{m_1+1}$ bzw. $\sigma = 2^{m_1}$. — Nennen wir $P(x)$ ein erzeugendes Polynom von $\mathfrak{K}$ über $\mathfrak{K}_0$, falls $\mathfrak{K}$ zum Restklassenkörper $\mathfrak{K}_0[x]/P(x)$ isomorph ist, so ist die Anzahl der Automorphismen von $\mathfrak{K}$ über $\mathfrak{K}_0$ gleich der Anzahl aller der Nullstellen α eines erzeugenden Polynoms $Q(x)$, für die $\mathfrak{K} = \mathfrak{K}_0(\alpha)$ wird. Aus dieser Bemerkung ergibt sich mühelos, daß Satz 7 und Satz 8 zusammengenommen gleichwertig sind mit dem folgenden Theorem:

Satz 9. Ist $P(x)$ ein erzeugendes Polynom des maximalen r.R.-Körpers $\mathfrak{K}$, so ist die Anzahl der reellen Nullstellen von $P(x)$ eine Potenz von 2 und es wird $\mathfrak{K} = \mathfrak{K}_0(\alpha)$ für jede reelle Nullstelle α von $P(x)$.

---

[14]) Über den Exponenten m läßt sich vermutlich keine genauere Aussage machen, abgesehen davon, daß trivialerweise $m = 0$, wenn $[\mathfrak{K}:\mathfrak{K}_0] \not\equiv 0\,(2)$ und $m \geqq 1$, wenn $[\mathfrak{K}:\mathfrak{K}_0] \equiv 0\,(2)$. Sicher ist *nicht* allgemein 2^m gleich der höchsten in $[\mathfrak{K}:\mathfrak{K}_0]$ aufgehenden Potenz von 2. Beispiel: $\mathfrak{K}_0$ der Körper der rationalen Zahlen, $\alpha = +\sqrt{1+\sqrt{3}}$, $\beta = +\sqrt{1-\sqrt{3}}$. Hier ist, da β komplex, $\mathfrak{K}_0(\alpha) = \mathfrak{K}$ der maximale r.R.-Körper des Normalkörpers $\mathfrak{N} = \mathfrak{K}_0(\alpha, \beta)$, — ($[\mathfrak{K}_0(\alpha, \beta):\mathfrak{K}_0] = 8$ beachten!) —, und es ist $[\mathfrak{K}_0(\alpha):\mathfrak{K}_0] = 4$. Aber $\mathfrak{K}$ hat über $\mathfrak{K}_0$ nur zwei Automorphismen (charakterisiert durch $\alpha \to \alpha$ und $\alpha \to -\alpha$) und daneben zwei Isomorphismen auf einen echt konjugierten Körper (charakterisiert durch $\alpha \to \beta$ und $\alpha \to -\beta$).

Mit Satz 9 ist der Anschluß an die ältere Ausdrucksweise hergestellt, die lieber mit den erzeugenden Polynomen bzw. definierenden Gleichungen als mit den Körpern operiert. Man beachte aber, daß die Beweise durch die Hereinziehung der erzeugenden Polynome nur unnötig schwerfällig würden. Aus Satz 9 folgt insbesondere: Ein erzeugendes Polynom $P(x)$ des maximalen r.R.-Körpers $\mathfrak{K}$ besitzt dann und nur dann genau *eine* reelle Nullstelle, wenn $[\mathfrak{K}:\mathfrak{K}_0]$ ungerade ist. — Bei ungeradem Grad kann man übrigens die Forderung der Maximalität etwas abschwächen. Wir wollen kurz sagen, der Körper $\mathfrak{K}$ besitze (über seinem Grundkörper $\mathfrak{K}_0$) eine *Primkette*, wenn eine Körperfolge $\mathfrak{K}_0 \subset \mathfrak{K}_1 \subset \cdots \subset \mathfrak{K}_m = \mathfrak{K}$ existiert, bei der alle Relativgrade $[\mathfrak{K}_i:\mathfrak{K}_{i-1}]$ Primzahlen sind. Nach Satz 2 hat jeder maximale r.R.-Körper Primketten, aber natürlich gibt es auch r.R.-Körper mit Primkette, die nicht maximal sind. Eine nicht triviale Ergänzung von Satz 9 ist daher Satz 10:

Satz 10. Besitzt der r.R.-Körper $\mathfrak{K}$ eine Primkette und ist außerdem $[\mathfrak{K}:\mathfrak{K}_0]$ ungerade, so hat jedes erzeugende Polynom $P(x)$ von $\mathfrak{K}$ genau eine reelle Nullstelle.

Zum Beweise von Satz 10 beachte man: a) Die Behauptung läßt sich auch so formulieren: Alle echt konjugierten Körper von $\mathfrak{K}$ sind komplex und es gibt keinen echten Automorphismusvon $\mathfrak{K}$ über $\mathfrak{K}_0$. b) Unsere Behauptung ist nach Hilfssatz 2 richtig, wenn $[\mathfrak{K}:\mathfrak{K}_0]$ Primzahl. Ist daher $\mathfrak{K}_0 \subset \mathfrak{K}_1 \subset \cdots \subset \mathfrak{K}_m = \mathfrak{K}$ eine Primkette von $\mathfrak{K}$ über $\mathfrak{K}_0$, so dürfen wir nach Induktionsprinzipien annehmen, daß sie [in der Fassung a)] sowohl für $\mathfrak{K}_1$ über $\mathfrak{K}_0$ als auch für $\mathfrak{K}$ über $\mathfrak{K}_1$ zutrifft. Daraus ergibt sich aber sofort die Gültigkeit der Behauptung für $\mathfrak{K}$ über $\mathfrak{K}_0$. Satz 10 ist eine unmittelbare Verallgemeinerung von Hilfssatz 2, der den Fall erledigt, daß eine nur aus zwei Gliedern ($\mathfrak{K}_0$ und $\mathfrak{K}$) bestehende Primkette existiert. Dagegen läßt sich Hilfssatz 2 nur mit einigem Zwang als Spezialfall von Satz 9 auffassen — ein r.R.-Körper vom Primzahlgrad über dem Grundkörper braucht ja nicht maximal zu sein. Da aber der direkte Beweis von Hilfssatz 2 äußerst einfach ist[15]) brauchen wir auf diesen Punkt nicht näher einzugehen. — Natürlich liegt es nahe, zu fragen: Gilt etwa Satz 10 auch dann noch, wenn man auf die Existenz einer Primkette verzichtet und nur $[\mathfrak{K}:\mathfrak{K}_0] \not\equiv 0 (2)$ fordert? Ehe man hier eine unmittelbare Entscheidung anstrebt, wird man am besten zuerst ein Beispiel für einen r.R.-Körper $\mathfrak{K}$ suchen, der keine Primkette besitzt, obwohl der Grad $[\mathfrak{K}:\mathfrak{K}_0]$ ungerade ist. Ein solches Beispiel dürfte wesentlich mühsamer zu bilden sein, als das in § 1 angegebene Beispiel für einen r.R.-Körper ohne Primkette

[15]) Es verdient Erwähnung, daß beim Beweise von Hilfssatz 2 keine speziellen Eigenschaften der Binome und vor allem nicht die Einheitswurzeln gebraucht werden. Man überlegt so: Es sei $P(x)$ ein irreduzibles Polynom über dem reellen Körper $\mathfrak{K}_0$ vom Primzahlgrad $p \neq 2$ mit auflösbarer Gruppe und es sei $P(x)$ noch über dem reellen Körper $\mathfrak{K}_1 \supseteq \mathfrak{K}_0$ irreduzibel, während $P(x)$ über $\mathfrak{K}_1(\beta_0)$ reduzibel wird, wobei β_0 über $\mathfrak{K}_1$ reelle Nullstelle des irreduzibeln Polynoms $Q(x)$ vom Primzahlgrade q ist und $Q(x)$ außer β_0 nur komplexe Nullstellen $\beta_1, \ldots, \beta_{q-1}$ besitzt. Dann spaltet $P(x)$ wegen der Auflösbarkeit seiner Gruppe über $\mathfrak{K}_1(\beta_0)$ einen reellen Linearfaktor ab und man hat daher: $p = q$; $\alpha_0 = \sum_{k=0,\ldots,p-1} c_k \cdot \beta_0^k = c(\beta_0)$ $(c_k \in \mathfrak{K}_1)$, während $\alpha_i = c(\beta_i)$ $(i = 1, \ldots, q-1)$ die übrigen Nullstellen von $P(x)$ sind. Wäre nun etwa α_1 reell, $\alpha_1 = \overline{\alpha}_1$ und $\beta_1 = \overline{\beta}_i$ $(i \neq 1!)$, so hätte man $\alpha_1 = c(\beta_1) = \overline{\alpha}_1 = c(\overline{\beta}_1) = c(\beta_i) = \alpha_i$, was unmöglich.

mit $[\mathfrak{K}:\mathfrak{K}_0]=4$. Auch besteht immerhin die entfernte Möglichkeit, daß man hier auf eine Ausnahmestellung der Primzahl 2 stößt, wie sie bei unseren bisherigen Betrachtungen schon öfters hervortrat. Hier können wir diese Fragen auf sich beruhen lassen. Denn ein Vergleich des Beweises von Satz 10 mit dem Beweis von Satz 7 zeigt, daß man durch die Forderung $[\mathfrak{K}:\mathfrak{K}_0] \not\equiv 0 (2)$ den wirklich interessanten, in der allgemeinen Theorie der r.R.-Körper auftretenden Schwierigkeiten aus dem Wege geht.

Dagegen soll kurz durch ein Beispiel gezeigt werden, daß ohne einschränkende Annahmen über $[\mathfrak{K}:\mathfrak{K}_0]$ Satz 7 und 9 *nur* für *maximale* r.R.-Körper ausgesprochen werden können. Wir betrachten über dem Körper $\mathfrak{K}_0$ der rationalen Zahlen das Polynom $p(x)=x^6+6\cdot x^3-63\cdot x^2+9$. Über $\mathfrak{K}_1=\mathfrak{K}_0(\sqrt{7})$ zerfällt $p(x)$ in die Faktoren $p_1(x)=x^3+3\cdot\sqrt{7}\cdot x+3$, $p_2(x)=x^3-3\cdot\sqrt{7}\cdot x+3$. Da in der Hauptordnung aller ganzen algebraischen Zahlen des Körpers $\mathfrak{K}_1$ das Hauptideal (3) keinen Primidealfaktor in höherer als erster Potenz enthält, sind $p_1(x)$ und $p_2(x)$ nach SCHÖNEMANN-EISENSTEIN über $\mathfrak{K}_1$ irreduzibel, und daraus folgt sofort die Irreduzibilität von $p(x)$ über $\mathfrak{K}_0$. Das Polynom dritten Grades $p_1(x)$ besitzt genau *eine* reelle Nullstelle ϱ, und es ist daher $\mathfrak{K}_0(\varrho,\sqrt{7})$ r.R.-Körper über $\mathfrak{K}_1=\mathfrak{K}_0(\sqrt{7})$ und damit auch über $\mathfrak{K}_0$. Ferner hat man: $[\mathfrak{K}_0(\varrho):\mathfrak{K}_0]=6$, $[\mathfrak{K}_1(\varrho):\mathfrak{K}_0]=[\mathfrak{K}_1(\varrho):\mathfrak{K}_1]\cdot[\mathfrak{K}_1:\mathfrak{K}_0]=3\cdot 2=6$, also $\mathfrak{K}_1(\varrho)=\mathfrak{K}_0(\varrho,\sqrt{7})=\mathfrak{K}_0(\varrho)$. Es ist also $\mathfrak{K}_0(\varrho)$ ein r.R.-Körper über $\mathfrak{K}_0$ mit Primkette. Aber $p_2(x)$ hat drei reelle Nullstellen $\sigma_1,\sigma_2,\sigma_3$ und es sind daher nach Hilfssatz 2 die zu $\mathfrak{K}_0(\varrho)$ über $\mathfrak{K}_0$ konjugierten reellen Körper $\mathfrak{K}_0(\sigma_i)$ keine r.R.-Körper über $\mathfrak{K}_1$ und damit auch keine über $\mathfrak{K}_0$. Wir können daher feststellen:

Es gibt r.R.-Körper mit Primkette, die echt konjugierte reelle Körper besitzen, und zwar sogar solche, die ihrerseits keine r.R.-Körper über dem gegebenen Grundkörper sind[16]).

Der letzte Teil dieses Resultats ist besonders wichtig. Denn der Beweis des Konjugiertensatzes 7 wäre trivial gewesen, wenn man hätte zeigen können: Jeder zu einem r.R.-Körper konjugierte Körper muß selbst ein r.R.-Körper sein. — Nachdem aber diese Vermutung widerlegt ist, hat man den Eindruck, daß der Beweis von Satz 7 kaum wesentlich abgekürzt werden kann, und daß vor allem ein sorgfältiger Induktionsschluß nicht zu vermeiden ist.

[16]) Daß in unserem Beispiel die Anzahl der reellen Nullstellen von $p(x)$ $4=2^2$ ist uninteressant, da es ja auf die Zahl *der* reellen Nullstellen ankommt, die den Körper $\mathfrak{K}$ erzeugen. Es wäre übrigens wohl nicht schwer, ein Beispiel zu konstruieren, in dem die Zahl aller reellen Nullstellen keine zweier Potenz würde. Man müßte dazu über dem Körper $\mathfrak{K}_0$ der rationalen Zahlen das irreduzible Polynom $p(x)$ vom Grade 10 so bestimmen, daß $p(x)$ über $\mathfrak{K}_0(\sqrt{d})$ $(d>0)$ in zwei irreduzible Faktoren $p_1(x)$, $p_2(x)$ des Grades 5 zerfällt, wobei $p_1(x)$ eine, $p_2(x)$ dagegen fünf reelle Nullstellen besitzt. [Eine rechnerische Erschwerung für die Konstruktion liegt nur darin, daß man hier $p_1(x)$ und $p_2(x)$ nicht trinomisch annehmen kann.]

Bonn, Mathematisches Institut der Universität

(Eingegangen am 24. Oktober 1955)

NAUMANN, H.
Math. Zeitschr. Bd. 65, S. 91—103 (1956)

Beliebige konvexe Polytope als Schnitte und Projektionen höherdimensionaler Würfel, Simplizes und Maßpolytope*)

Von
HERBERT NAUMANN

In dieser Arbeit wird gezeigt, daß sich jedes konvexe Polytop als Schnitt eines höherdimensionalen Würfels und als Projektion eines höherdimensionalen Maßpolytops auffassen läßt. Für Mittelpunktspolytope ist speziell eine Darstellung als Mittelpunktsschnitt bzw. senkrechte Parallelprojektion möglich. Ebenfalls wird die Darstellbarkeit beliebiger konvexer Polytope als Schnitt und Projektion höherdimensionaler regulärer Simplizes gezeigt. Es werden Abschätzungen für die Dimension des höherdimensionalen Würfels usw. gegeben.

1. Sei zunächst in einem n-dimensionalen euklidischen Raum ein *konvexes Polytop mit Mittelpunkt* gegeben. Wir wollen voraussetzen, daß ein Polytop mindestens einen inneren Punkt besitzen soll. Folglich ist dann der diametral gelegene Punkt ebenfalls ein innerer Punkt, und damit wegen der Konvexität auch der Mittelpunkt des Polytops innerer Punkt. Der Mittelpunkt liege im Koordinatenursprung. Dann lassen sich die $2m$ extremen Stützen des gegebenen Polytops analytisch in der Normalform

$$\left.\begin{aligned} a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n &= +1 \\ a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n &= -1 \end{aligned}\right\} \quad (i = 1, 2, \ldots, m) \tag{1}$$

darstellen. Die Punkte des von den extremen Stützen eingeschlossenen Raums genügen ersichtlich der Beziehung

$$\max_{i=1}^{m} \left| \sum_{k=1}^{n} a_{ik} x_k \right| \leqq 1, \tag{2}$$

wobei das Gleichheitszeichen genau auf dem Rande gilt. Es läßt sich also jedes konvexe Mittelpunktspolytop (genauer: sein Rand) durch eine Gleichung

$$\max_{i=1}^{m} \left| \sum_{k=1}^{n} a_{ik} x_k \right| = 1 \tag{3}$$

darstellen. Umgekehrt stellt eine Gleichung der Gestalt (3) genau dann den Rand eines konvexen Mittelpunktspolytops dar, wenn das Gebilde nur Punkte

*) Für Unterstützung dieser Arbeit sage ich der Deutschen Forschungsgemeinschaft meinen aufrichtigen Dank.

im Endlichen besitzt, d.h. wenn nach Einführung homogener Koordinaten $\bar{x}_k = \bar{x}_0 x_k$ die Gleichung

$$\max_{i=1}^{m} \left| \sum_{k=1}^{n} a_{ik} \bar{x}_k \right| = 0 \tag{4}$$

keine nichttriviale Lösung besitzt. Da dies äquivalent damit ist, daß das homogene Gleichungssystem

$$\sum_{k=1}^{n} a_{ik} \bar{x}_k = 0 \qquad (i = 1, \ldots, m) \tag{5}$$

keine nichttriviale Lösung besitzt, so ergibt sich als notwendige und hinreichende Bedingung dafür, daß das Gebilde (3) beschränkt ist, daß die Matrix $((a_{ik}))$ vom Range $\varrho = n$ ist. Konvexes Polytop ist sodann das von (3) berandete Gebilde als beschränkter Durchschnitt endlich vieler Stützstreifen.

Sei nun ein *beliebiges konvexes Polytop* des R_n gegeben. Die m extremen Stützen seien

$$\sum_{k=1}^{n} a_{ik} x_k = a_i, \qquad i = 1, \ldots, m. \tag{6}$$

Dann läßt sich zu jedem a_i ein $\bar{a}_i$ finden mit der Eigenschaft, daß das Polytop ganz zwischen der Hyperebene $\sum_{k=1}^{n} a_{ik} x_k = a_i$ und der Hyperebene $\sum_{k=1}^{n} a_{ik} x_k = \bar{a}_i$ liegt. Nach Subtraktion von $\frac{a_i + \bar{a}_i}{2}$ von beiden Seiten beider Gleichungen und anschließende Division durch $\frac{a_i - \bar{a}_i}{2}$ erhalten wir, daß sich jede extreme Stütze $\sum_{k=1}^{n} a_{ik} x_k = a_i$ derart in der Form $a_i' + \sum_{k=1}^{n} a_{ik}' x_k = 1$ schreiben läßt, daß das Polytop ganz zwischen $a_i' + \sum_{k=1}^{n} a_{ik}' x_k = +1$ und $a_i' + \sum_{k=1}^{n} a_{ik}' x_k = -1$ liegt. Ganz entsprechend wie bei den Mittelpunktspolytopen ergibt sich daraus

Satz 1.1. *Jedes konvexe Polytop des R_n mit m extremen Stützen läßt sich in der Form*

$$\max_{i=1}^{m} \left| a_i + \sum_{k=1}^{n} a_{ik} x_k \right| = 1 \tag{7}$$

darstellen.

Es bilden auch umgekehrt die Punkte, die einer Gleichung der Gestalt (7) genügen, genau dann den Rand eines konvexen Polytops, wenn es einen Punkt $(\xi_1, \xi_2, \ldots, \xi_n)$ gibt, für den $\max_{i=1}^{m} \left| a_i + \sum_{k=1}^{n} a_{ik} \xi_k \right| < 1$ ist und die Matrix $((a_{ik}))$ vom Range $\varrho = n$ ist. Die erstere Bedingung brauchte im Falle der Mittelpunktspolytope nicht besonders angegeben werden, da in der Darstellung (3) der Punkt $(0, 0, \ldots, 0)$ stets ein innerer Punkt ist. Die zweite Bedingung ergibt sich entsprechend wie bei den Mittelpunktspolytopen.

2. Eine ganz analoge Darstellung ergibt sich bei Verwendung von Hyperebenenkoordinaten.

Seien die p Ecken eines konvexen Polytops durch ihre Punktkoordinaten

$$(a_{i1}, a_{i2}, \ldots, a_{in}) \qquad i = 1, \ldots, p \tag{1}$$

gegeben und der Punkt $(0, 0, \ldots, 0)$ ein innerer Punkt des Polytops. Durch die spezielle Polarkorrelation

$$x_k^* = u_k, \qquad u_k^* = x_k \qquad (k = 1, \ldots, n), \tag{2}$$

wobei die u_k als Koordinaten der Hyperebene

$$\sum_{k=1}^{n} u_k x_k = 1 \tag{3}$$

aufzufassen sind, geht das Polytop wieder in ein konvexes Polytop über, das den Punkt $(0, 0, \ldots, 0)$ als inneren Punkt besitzt. Die Ecken des ursprünglichen Polytops sind hierbei in die extremen Stützen

$$\sum_{k=1}^{n} a_{ik} x_k^* = 1, \qquad i = 1, \ldots, p \tag{4}$$

des transformierten Polytops übergegangen. Nach Satz 1.1 läßt sich dieses in der Form

$$\max_{i=1}^{p} \left| b_i + \sum_{k=1}^{n} b_{ik} x_k^* \right| = 1 \tag{5}$$

darstellen. Macht man nun die Korrelation (2) wieder rückgängig, so ergibt sich

$$\max_{i=1}^{p} \left| b_i + \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \tag{6}$$

als Darstellung des ursprünglich gegebenen Polytops in Hyperebenenkoordinaten, und zwar genügen der Gl. (6) genau die Hyperebenen, die das Polytop umhüllen und mindestens einen Punkt mit seinem Rand gemeinsam haben.

Satz 2.1. *Jedes konvexe Polytop des R_n mit p Ecken läßt sich in der Form*

$$\max_{i=1}^{p} \left| b_i + \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \tag{7}$$

darstellen.

Es ergibt sich unmittelbar, daß sich jedes konvexe Mittelpunktspolytop mit $2p$ Ecken in der Form

$$\max_{i=1}^{p} \left| \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \tag{8}$$

darstellen läßt, wo

$$\left.\begin{array}{c} (b_{i1}, b_{i2}, \ldots, b_{in}) \\ (-b_{i1}, -b_{i2}, \ldots, -b_{in}) \end{array}\right\} \qquad i = 1, \ldots, p$$

die Ecken des Polytops in Punktkoordinaten sind.

3. Wir betrachten nun eine spezielle Klasse konvexer Polytope, die hier „Hauptpolytope" genannt seien.

Definition. Ein Hauptpolytop ist ein Polytop, welches bei geeigneter Lage im Koordinatensystem folgende Symmetrieeigenschaften besitzt:

Mit $(a_1, a_2, \ldots, a_{n-1}, a_n)$ sind auch $(a_2, a_3, \ldots, a_n, a_1)$ und $(-a_1, a_2, \ldots, a_{n-1}, a_n)$ Punkte des Polytops.

Offenbar ist diese Bedingung zu jeder der beiden folgenden Bedingungen äquivalent:

a) Mit $b_1 x_1 + b_2 x_2 + \cdots + b_{n-1} x_{n-1} + b_n x_n = 1$ sind auch $b_2 x_1 + b_3 x_2 + \cdots + b_n x_{n-1} + b_1 x_n = 1$ und $-b_1 x_1 + b_2 x_2 + \cdots + b_{n-1} x_{n-1} + b_n x_n = 1$ extreme Stützen des Polytops.

b) Mit $(a_1, a_2, \ldots, a_{n-1}, a_n)$ sind auch $(a_2, a_3, \ldots, a_n, a_1)$ und $(-a_1, a_2, \ldots, a_{n-1}, a_n)$ Eckpunkte des Polytops.

Da die beiden letzten Bedingungen dual zueinander sind, so ist das zu einem Hauptpolytop polare Polytop wieder ein Hauptpolytop.

Beispiele für Hauptpolytope sind alle regulären Polytope mit Ausnahme der Simplizes und der regulären $(4k+1)$-, $(4k+2)$- und $(4k+3)$-Ecke, weitere Beispiele sind Kubooktaeder, Rhombendodekaeder, Triakisoktaeder, Tetrakishexaeder usw.

Bringt man ein Hauptpolytop mit $2m$ extremen Stützen und $2p$ Ecken nach dem in § 1 bzw. § 2 beschriebenen Verfahren auf die Gestalt (1.3) bzw. (2.8), so genügen dann die Koeffizienten a_{ik} bzw. b_{ik} den „Orthogonalitätsrelationen"

$$\sum_{i=1}^{m} a_{ik} a_{il} = \begin{cases} c & \text{für } k = l \\ 0 & \text{für } k \neq l \end{cases} \qquad (k, l = 1, \ldots, n) \tag{1}$$

bzw.

$$\sum_{i=1}^{p} b_{ik} b_{il} = \begin{cases} c' & \text{für } k = l \\ 0 & \text{für } k \neq l \end{cases} \qquad (k, l = 1, \ldots, n). \tag{2}$$

Wir begnügen uns mit dem Nachweis von (1), da der Nachweis von (2) analog verläuft. Die Koeffizientenmatrix des gegebenen Hauptpolytops ist

$$\mathfrak{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Nach der Bedingung a) für Hauptpolytope müssen die Polytope mit den Koeffizientenmatrizen

$$\mathfrak{A}_1 = \begin{pmatrix} a_{12} & a_{13} & \ldots & a_{1n} & a_{11} \\ a_{22} & a_{23} & \ldots & a_{2n} & a_{21} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m2} & a_{m3} & \ldots & a_{mn} & a_{m1} \end{pmatrix}, \qquad \mathfrak{A}_2 = \begin{pmatrix} -a_{11} & a_{12} & \ldots & a_{1n} \\ -a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

mit dem gegebenen Polytop identisch sein. Da die Hyperebenen $\sum_{k=1}^{n} a_{ik} x_k = 1$ $(i = 1, \ldots, m)$ umkehrbar eindeutig den $2m$ extremen Stützen des Polytops zugeordnet sind, so entstehen also die Zeilen von $\mathfrak{A}_1$ und die Zeilen von $\mathfrak{A}_2$ durch eine Umordnung der Zeilen von $\mathfrak{A}$ unter eventueller Multiplikation aller Glieder einer Zeile mit -1. Folglich ist die Quadratsumme der Glieder einer Spalte für alle Spalten konstant und $\sum_{i=1}^{m} a_{i1} a_{il} = \sum_{i=1}^{m} (-a_{i1}) a_{il} = 0$ für $l = 2, \ldots, n$, woraus durch wiederholte Anwendung der Eigenschaften eines Hauptpolytops schließlich folgt, daß die Spaltenvektoren aus $\mathfrak{A}$ paarweise orthogonal zueinander sind, womit der Beweis unserer Behauptung vollständig erbracht ist.

4. In diesem Paragraphen zeigen wir:

Satz 4.1. *Jedes Mittelpunktspolytop des R_n, das eine Darstellung*

$$(1) \qquad \max_{i=1}^{m} \left| \sum_{k=1}^{n} a_{ik} x_k \right| = 1 \quad \text{mit} \quad \sum_{i=1}^{m} a_{ik} a_{il} = \begin{cases} c & \text{für } k = l \\ 0 & \text{für } k \neq l \end{cases} \quad (k, l = 1, \ldots, n)$$

besitzt, läßt sich als Mittelpunktsschnitt eines m-dimensionalen Würfels mit einem n-dimensionalen linearen Raum darstellen.

Satz 4.2. *Jedes Mittelpunktspolytop des R_n, das eine Darstellung*

$$(2) \qquad \max_{i=1}^{p} \left| \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \quad \text{mit} \quad \sum_{i=1}^{p} b_{ik} b_{il} = \begin{cases} c' & \text{für } k = l \\ 0 & \text{für } k \neq l \end{cases} \quad (k, l = 1, \ldots, n)$$

besitzt, läßt sich als senkrechte Parallelprojektion eines p-dimensionalen Maßpolytops auf einen n-dimensionalen linearen Raum darstellen.

Mit den Ergebnissen von § 3 ergibt sich hieraus als unmittelbare Folgerung:

Satz 4.3. *Jedes konvexe Hauptpolytop, das von $2m$ extremen Stützen begrenzt wird und $2p$ Ecken besitzt, ist als Mittelpunktsschnitt des m-dimensionalen Würfels und als senkrechte Parallelprojektion des p-dimensionalen Maßpolytops darstellbar.*

Zum Beweis von Satz 4.1 setzen wir

$$(3) \qquad d_{ik} = \frac{a_{ik}}{\sqrt{c}} \quad (i = 1, \ldots, m, \; k = 1, \ldots, n).$$

Die Spaltenvektoren der Matrix $((d_{ik}))$ bilden dann n normierte Einheitsvektoren mit m Komponenten, es läßt sich also die Matrix $((d_{ik}))$ durch Hinzufügen von $m - n$ weiteren Spalten zu einer orthogonalen m-reihigen Matrix erweitern. Der m-dimensionale Würfel der Kantenlänge $\frac{2}{\sqrt{c}}$ läßt sich bekanntlich in der Form

$$(4) \qquad \max_{i=1}^{m} \left| \sqrt{c}\, x_i' \right| = 1$$

und nach Anwendung der orthogonalen Substitution

$$x_i' = \sum_{k=1}^{m} d_{ik} x_k \qquad (i = 1, \ldots, m) \tag{5}$$

folglich auch in der Form

$$\max_{i=1}^{m} \left| \sum_{k=1}^{m} c d_{ik} x_k \right| = 1 \tag{6}$$

darstellen. Durch Schnitt dieses Würfels mit dem n-dimensionalen linearen Raum $x_{n+1} = x_{n+2} = \cdots = x_m = 0$ ergibt sich mittels (3) in der Tat das gegebene Polytop.

Der Beweis von Satz 4.2 folgt hieraus durch Dualisierung.

5. Aus dem Satz 4.3 für konvexe Hauptpolytope leiten wir nun einen Beweis des Satzes her, daß sich jedes beliebige konvexe Polytop als Schnitt eines höherdimensionalen Würfels und als Projektion eines höherdimensionalen Maßpolytops darstellen läßt, und geben gleichzeitig eine Abschätzung für die Dimensionszahl des höherdimensionalen Würfels bzw. Maßpolytops.

Wir betrachten im R_n irgendeine Hyperebene

$$\sum_{i=1}^{n} a_i x_i = 1, \tag{1}$$

wobei die Koeffizienten a_i ihrem absoluten Betrag nach paarweise untereinander und von Null verschieden seien. Durch wiederholte Anwendung der Symmetrieoperationen, die Hauptpolytope invariant lassen, wird von der Hyperebene (1) ein Hauptpolytop mit den extremen Stützen

$$\sum_{i=1}^{n} (-1)^{\mu_i} a_{i+\nu_i} x_i = 1 \qquad (\mu_i = 0, 1,\ \nu_i = 0, \ldots, n-1;\ \text{Indizes mod } n) \tag{2}$$

erzeugt; die Anzahl dieser extremen Stützen beträgt nach der Voraussetzung über die a_i genau $2^n \cdot n$.

Bringt man nun im Inneren eines der $(n-1)$-dimensionalen Begrenzungspolytope des soeben konstruierten Hauptpolytops ein beliebiges konvexes Polytop des R_{n-1}, welches p Ecken besitzen möge, unter (eventuell nach entsprechender Streckung des Hauptpolytops), überträgt dieses durch Anwendung der erwähnten Symmetrieoperationen auf die $2^n \cdot n - 1$ übrigen Begrenzungspolytope des Hauptpolytops und bildet die konvexe Hülle des $(n-1)$-dimensionalen Polytops und seiner $2^n \cdot n - 1$ Bilder, so entsteht ein (dem ursprünglichen Hauptpolytop einbeschriebenes) konvexes Hauptpolytop mit $2^n \cdot n \cdot p$ Ecken, das unter seinen $(n-1)$-dimensionalen Begrenzungspolytopen $2^n \cdot n$ dem vorgegebenen konvexen Polytop des R_{n-1} kongruente Polytope enthält.

Nach Satz 4.3 ist das zuletzt gefundene Hauptpolytop als Projektion des $(2^{n-1} \cdot n \cdot p)$-dimensionalen Maßpolytops darstellbar. Legt man nun durch eines der oben erwähnten Begrenzungspolytope mit p Ecken einen $(n-1)$-

dimensionalen Raum als Projektionsraum, so wird das Hauptpolytop von einem außerhalb und genügend nahe über dem zugehörigen Begrenzungspolytop gelegenen Projektionszentrum auf dieses Begrenzungspolytop projiziert. Da die Projektion einer Projektion wieder eine Projektion liefert, so ist damit, wenn man n durch $n+1$ ersetzt, erhalten:

Satz 5.1. *Jedes beliebige konvexe Polytop des R_n mit p Ecken ist als Projektion eines $(2^n \cdot (n+1) \cdot p)$-dimensionalen Maßpolytops darstellbar.*

Das Dualitätsprinzip liefert hierzu:

Satz 5.2. *Jedes beliebige konvexe Polytop des R_n mit m extremen Stützen ist als Schnitt eines $(2^n \cdot (n+1) \cdot m)$-dimensionalen Würfels darstellbar.*

6. Wir entwickeln nun auf einem anderen Wege eine Abschätzung für den Würfelschnittsatz und den hierzu dualen Satz speziell für Mittelpunktspolytope.

Sei ein beliebiges konvexes Mittelpunktspolytop

$$\max_{i=1}^{p} \left| \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \tag{1}$$

gegeben. Wir setzen jetzt

$$\mathfrak{r}_i = \begin{pmatrix} b_{i1} \\ b_{i2} \\ \vdots \\ b_{in} \end{pmatrix} \quad (i = 1, \ldots, p), \tag{2}$$

$$\mathfrak{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \tag{3}$$

und führen den Richtungsvektor

$$\mathfrak{c} = \begin{pmatrix} \cos \alpha_1 \\ \cos \alpha_2 \\ \vdots \\ \cos \alpha_n \end{pmatrix} = \frac{\mathfrak{x}}{|\mathfrak{x}|} = \frac{\mathfrak{x}}{R} \tag{4}$$

ein. Man erkennt, daß (1) die konvexe Hülle der Punkte $\pm \mathfrak{r}_i$ ist. Der Ausdruck

$$J = \sum_{i=1}^{p} (\mathfrak{r}_i^T \mathfrak{c})^2 \tag{5}$$

läßt sich als „Trägheitsmoment" bezüglich der zur Richtung $\mathfrak{c}$ orthogonalen Hyperebene $\mathfrak{c}^T \mathfrak{x} = 0$ bezeichnen. Es ist

$$\begin{aligned} J &= \sum_{i=1}^{p} \left(\sum_{k=1}^{n} b_{ik} \cos \alpha_k \right)^2 \\ &= \sum_{i=1}^{p} \sum_{k,l=1}^{n} b_{ik} b_{il} \cos \alpha_k \cos \alpha_l \\ &= \sum_{k,l=1}^{n} \left(\sum_{i=1}^{p} b_{ik} b_{il} \right) \cos \alpha_k \cos \alpha_l . \end{aligned}$$

Damit geht (5) über in

$$J = \sum_{k,l=1}^{n} J_{kl} \cos \alpha_k \cos \alpha_l, \tag{6}$$

wo

$$J_{kl} = \sum_{i=1}^{p} b_{ik} b_{il} \quad (k, l = 1, \ldots, n) \tag{7}$$

gesetzt ist. Trägt man nun in jeder Richtung c den Vektor der Länge

$$R = \frac{1}{\sqrt{J}} \tag{8}$$

ab, wo J das zur Richtung c gehörige Trägheitsmoment ist, so genügen die Endpunkte dieser Vektoren der Beziehung

$$J = \frac{1}{R^2} = \sum_{k,l=1}^{n} J_{kl} \frac{x_k x_l}{R^2}, \tag{9}$$

d.h. sie erfüllen die Hyperfläche zweiter Ordnung

$$\sum_{k,l=1}^{n} J_{kl} x_k x_l = 1, \qquad J_{kl} = \sum_{i=1}^{p} b_{ik} b_{il}. \tag{10}$$

Diese Fläche läßt sich durch eine orthogonale Substitution der x_i stets auf Hauptachsen transformieren, wobei die Punkte $\pm r_i$ entsprechend mittransformiert werden. Wir haben also erhalten:

Satz 6.1. *Jedes konvexe Mittelpunktspolytop läßt sich durch eine Gleichung*

$$\max_{i=1}^{p} \left| \sum_{k=1}^{n} b_{ik} u_k \right| = 1 \quad \text{mit} \quad \sum_{i=1}^{p} b_{ik} b_{il} = 0 \quad \text{für} \quad k \neq l \tag{11}$$

darstellen.

Durch Dualisierung erhält man:

Satz 6.2. *Jedes konvexe Mittelpunktspolytop läßt sich durch eine Gleichung*

$$\max_{i=1}^{m} \left| \sum_{k=1}^{n} a_{ik} x_k \right| = 1 \quad \text{mit} \quad \sum_{i=1}^{m} a_{ik} a_{il} = 0 \quad \text{für} \quad k \neq l \tag{12}$$

darstellen.

Man erkennt unmittelbar, daß man zu einem beliebigen konvexen Mittelpunktspolytop mit $2p$ Ecken weitere Paare symmetrisch zum Nullpunkt gelegener, im Inneren oder teilweise auf dem Rande befindlicher Punkte derart hinzunehmen kann, daß aus dem Trägheits-„ellipsoid" eine „Trägheitshyperkugel" entsteht. Dies bedeutet nach Satz 4.2, daß jedes konvexe Mittelpunktspolytop als senkrechte Parallelprojektion eines höherdimensionalen Maßpolytops darstellbar ist. Wir führen nun eine entsprechende Rechnung mit dem Ziel einer Abschätzung durch, und zwar zunächst für den dualen Fall.

Sei ein konvexes Mittelpunktspolytop gegeben, und zwar bereits in der „auf Hauptachsen transformierten" Form (12). Es möge das Maßpolytop $\sum_{i=1}^{n} |x_i| = r$ einschließen und von dem Würfel $\max_{i=1}^{n} |x_i| = R$ eingeschlossen werden. Wir betrachten die Koeffizientenmatrix $((a_{ik}))$. Nach Voraussetzung verschwinden die Summen $\sum_{i=1}^{m} a_{ik} a_{il}$ für $k \neq l$. Zur Abkürzung setzen wir $\sum_{i=1}^{m} a_{ik}^2 = A_k$ und nehmen ohne Beschränkung der Allgemeinheit an, daß $A_1 \geqq A_k$ für $k = 1, \ldots, n$ ist. Nach Definition von r folgt $|a_{ik}| \leq \frac{1}{r}$ für $i = 1, \ldots, m$, $k = 1, \ldots, n$, also $A_1 \leq \frac{m}{r^2}$. Sei nun

$$t = \left\lfloor m \cdot \frac{R^2}{r^2} \right\rfloor, \tag{13}$$

d.h. die kleinste natürliche Zahl t mit $t \geqq m \cdot \frac{R^2}{r^2}$. Dann ist

$$\max_{k=1}^{n} \left| \sqrt{\frac{A_1 - A_k}{t}} \cdot x_k \right| < \frac{\sqrt{\frac{m}{r^2}}}{\sqrt{\frac{m R^2}{r^2}}} \cdot R = 1 \tag{14}$$

für alle Punkte des gegebenen Polytops, folglich ist das Polytop

$$\max_{i=1}^{m+t(n-1)} \left| \sum_{k=1}^{n} a'_{ik} x_k \right| = 1 \tag{15}$$

mit

$$a'_{ik} = \begin{cases} a_{ik} & \text{für} \quad i = 1, \ldots, m, \; k = 1, \ldots, n \\ \sqrt{\frac{A_1 - A_k}{t}} & \text{für} \quad \begin{cases} k = 2, \ldots, n \\ i = m + (k-2)\,t + 1, \ldots, m + (k-1)\,t, \end{cases} \\ 0 & \text{in allen übrigen Fällen} \end{cases}$$

mit dem gegebenen Polytop identisch, und es ist

$$\sum_{i=1}^{m+t(n-1)} a'_{ik} a'_{il} = 0 \quad \text{für} \quad k \neq l, \; k, l = 1, \ldots, n,$$

$$\sum_{i=1}^{m+t(n-1)} a'^2_{i1} = \sum_{i=1}^{m} a^2_{i1} = A_1,$$

$$\sum_{i=1}^{m+t(n-1)} a'^2_{ik} = \sum_{i=1}^{m} a^2_{ik} + t \cdot \frac{A_1 - A_k}{t} = A_1 \quad \text{für} \quad k = 2, \ldots, n.$$

Folglich haben wir nach Satz 4.1 erhalten:

Satz 6.3. *Jedes konvexe Mittelpunktspolytop des R_n mit $2m$ extremen Stützen, das bei einer bestimmten Lage im Koordinatensystem das Maßpolytop $\sum_{i=1}^{n} |x_i| = r$ einschließt und von dem Würfel $\max_{i=1}^{n} |x_i| = R$ eingeschlossen wird,*

ist als Mittelpunktsschnitt des $(m+m\alpha^2\cdot(n-1))$*-dimensionalen Würfels darstellbar, wo* $\alpha \geqq \frac{R}{r}$ *und* $m\alpha^2$ *eine natürliche Zahl ist.*

Durch Dualisierung folgt hieraus:

Satz 6.4. *Jedes konvexe Mittelpunktspolytop des* R_n *mit* $2p$ *Ecken, das bei einer bestimmten Lage im Koordinatensystem das Maßpolytop* $\max_{i=1}^{n} |u_i| = R$ *einschließt und von dem Würfel* $\sum_{i=1}^{n} |u_i| = r$ *eingeschlossen wird, ist als senkrechte Parallelprojektion des* $(p+p\alpha^2\cdot(n-1))$*-dimensionalen Maßpolytops darstellbar, wo* $\alpha \geqq \frac{R}{r}$ *und* $p\alpha^2$ *eine natürliche Zahl ist.*

Auf dem in diesem Paragraphen beschrittenen Wege ließen sich auch entsprechende Abschätzungen für beliebige konvexe Polytope herleiten, da man z.B. jedes konvexe Polytop des R_n in einfacher Weise als Schnitt eines $(n+1)$-dimensionalen Mittelpunktspolytops darstellen kann. Wir wollen an dieser Stelle aber nicht näher darauf eingehen.

7. In diesem Paragraphen wird eine weitere analytische Darstellung konvexer Polytope gegeben.

Seien

$$\sum_{k=1}^{n} a_{ik} x_k - 1 = 0 \qquad (i = 1, \ldots, m) \tag{1}$$

die extremen Stützen eines konvexen Polytops; der Koordinatenursprung sei innerer Punkt des Polytops. Gesucht sind positive „Gewichte" $p_1, p_2, \ldots, p_m$, so daß

$$\sum_{i=1}^{m} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) \equiv \text{const} \tag{2}$$

ist für den gesamten n-dimensionalen Raum. Durch Umordnung dieses Ausdrucks ergibt sich

$$\sum_{k=1}^{n} \left(\sum_{i=1}^{m} p_i a_{ik} \right) x_k - \sum_{i=1}^{m} p_i \equiv \text{const}, \tag{3}$$

also

$$\sum_{i=1}^{m} p_i a_{ik} = 0 \qquad (k = 1, \ldots, n) \tag{4}$$

als Bedingungen für die p_i. Nun sind

$$\sum_{k=1}^{n} a_{ik} u_k = 1, \tag{5}$$

d.h. die Punkte mit den Koordinaten

$$(a_{i1}, a_{i2}, \ldots, a_{in}) \quad \text{mit} \quad i = 1, \ldots, m \tag{6}$$

die Ecken des zum ursprünglichen Polytop polaren Polytops, es ist wie das ursprüngliche konvex und besitzt den Koordinatenursprung als inneren

Punkt. Es ist daher der Punkt $(0, 0, \ldots, 0)$ als Schwerpunkt einer positiven Massenbelegung der Punkte (6) darstellbar, d.h. das Gleichungssystem (4) und damit auch die Beziehung (2) besitzen ein System positiver Lösungen p_i.

Nachdem die Existenz der positiven Lösungen p_i gezeigt ist, zeigen wir:

Satz 7.1. *Sind* $\sum_{k=1}^{n} a_{ik} x_k = 1$ $(i = 1, \ldots, m)$ *die extremen Stützen eines konvexen Polytops, das den Punkt* $(0, 0, \ldots, 0)$ *als inneren Punkt enthält, so lassen sich stets (im allgemeinen auf mehrfache Weise) positive Gewichte* p_i *finden, daß*

$$\frac{\sum_{i=1}^{m} \left| p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) \right|}{\sum_{i=1}^{m} p_i} = 1 \tag{7}$$

eine Darstellung der Randpunkte und inneren Punkte des gegebenen Polytops ist.

Beweis. Für Rand- und innere Punkte sind die linken Seiten der Gln. (1) nicht positiv, also ist, wenn man für die p_i ein System der oben gefundenen Gewichte einsetzt,

$$\sum_{i=1}^{m} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) = - \sum_{i=1}^{m} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) = \sum_{i=1}^{m} p_i \tag{8}$$

und die Gl. (7) folglich erfüllt. Für jeden äußeren Punkt gilt nach passender Umnumerierung der extremen Stützen

$$\sum_{k=1}^{n} a_{ik} x_k - 1 \quad \begin{cases} > 0 \text{ für } i = 1, \ldots, j & (j \geqq 1) \\ \leqq 0 \text{ für } i = j+1, \ldots, m, \end{cases} \tag{9}$$

also

$$\begin{aligned} \sum_{i=1}^{m} \left| p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) \right| &= \sum_{i=1}^{j} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) - \sum_{i=j+1}^{m} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) \\ &= - \sum_{i=1}^{m} p_i \left(\sum_{k=1}^{n} a_{ik} x_k - 1 \right) + 2 \sum_{i=1}^{j} p_i \left(\sum_{k=1}^{n} a_{ik} a_k - 1 \right) \\ &> \sum_{i=1}^{m} p_i, \end{aligned} \tag{10}$$

womit die Behauptung bewiesen ist.

Nach dem Dualitätsprinzip ergibt sich:

Satz 7.2. *Sind* $(b_{i1}, b_{i2}, \ldots, b_{in})$ *mit* $i = 1, \ldots, p$ *die Ecken eines konvexen Polytops, das den Punkt* $(0, 0, \ldots, 0)$ *als inneren Punkt enthält, so lassen sich stets positive Gewichte* p_i *finden, daß*

$$\frac{\sum_{i=1}^{p} \left| p_i \left(\sum_{k=1}^{n} b_{ik} u_k - 1 \right) \right|}{\sum_{i=1}^{p} p_i} = 1 \tag{11}$$

eine Darstellung der einhüllenden und meidenden Hyperebenen des gegebenen Polytops ist.

8. Die im letzten Paragraphen gewonnene Darstellung (7.7) werten wir in einem speziellen Falle weiter aus. Der n-dimensionale Würfel der Kantenlänge 2 läßt sich nach diesem Formalismus in der Gestalt

$$(1) \quad |1+x_1|+|1-x_1|+|1+x_2|+|1-x_2|+\cdots+|1+x_n|+|1-x_n| = 2n$$

darstellen. Die Beziehung (1) läßt sich aber auch unmittelbar einsehen. Es zeigt sich nun, daß dieser Würfel als Schnitt des $2n$-dimensionalen Maßpolytops

$$(2) \quad |y_1|+|y_2|+\cdots+|y_{2n}| = n\cdot\sqrt{2}$$

erhalten werden kann, und zwar als Schnitt eines der dieses Maßpolytop berandenden $(2n-1)$-dimensionalen Simplizes der Kantenlänge $2n$. Denn wendet man auf (2) die orthogonale Substitution

$$(3) \quad y_i = \begin{cases} \dfrac{x_i}{\sqrt{2}} + \dfrac{x_{n+i}}{\sqrt{2}} & \text{für} \quad i = 1,\ldots,n \\ -\dfrac{x_{i-n}}{\sqrt{2}} + \dfrac{x_i}{\sqrt{2}} & \text{für} \quad i = n+1,\ldots,2n \end{cases}$$

an und schneidet man das so transformierte Maßpolytop mit dem n-dimensionalen linearen Raum

$$x_{n+1} = x_{n+2} = \cdots = x_{2n} = 1,$$

so ergibt sich in der Tat der Würfel (1). Da der Gl. (1) außer den Randpunkten auch alle inneren Punkte des Würfels genügen, der Gl. (2) aber lediglich die Randpunkte des Maßpolytops, so folgt, daß (1) durch Schnitt eines Randpolytops von (2), also eines regulären $(2n-1)$-dimensionalen Simplex der Kantenlänge $2n$, dargestellt ist.

Der Schwerpunkt des Simplex mit den Ecken

$$\begin{aligned} \mathfrak{y}_1 &= \left(\frac{2n}{\sqrt{2}}, 0, \ldots, 0\right) \\ \mathfrak{y}_2 &= \left(0, \frac{2n}{\sqrt{2}}, \ldots, 0\right) \\ &\vdots \qquad\qquad \ddots \\ \mathfrak{y}_{2n} &= \left(0, 0, \ldots, \frac{2n}{\sqrt{2}}\right), \end{aligned}$$

also der Punkt $\mathfrak{y} = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, \ldots, \frac{1}{\sqrt{2}}\right)$, geht hierbei in den Mittelpunkt des Würfels über.

Es gilt also:

Satz 8.1. *Der n-dimensionale Würfel der Kantenlänge a läßt sich darstellen als Schnitt durch den Schwerpunkt eines $(2n-1)$-dimensionalen regulären Simplex der Kantenlänge $n\cdot a$ mit einem n-dimensionalen linearen Raum.*

Der hierzu duale Satz ist von P. H. SCHOUTE [2] § 8.84 (Theorem II) bewiesen worden.

Nach Satz 4.3 folgt:

Satz 8.2. *Jedes konvexe Hauptpolytop, das von $2m$ extremen Stützen begrenzt wird und $2p$ Ecken besitzt, ist als Schnitt durch den Schwerpunkt eines $(2m-1)$-dimensionalen regulären Simplex und als senkrechte Parallelprojektion eines $(2p-1)$-dimensionalen regulären Simplex darstellbar.*

Aus Satz 5.1 und Satz 5.2 ergibt sich:

Satz 8.3. *Jedes konvexe Polytop ist als Schnitt eines höherdimensionalen regulären Simplex und als Projektion eines höherdimensionalen regulären Simplex darstellbar.*

Aus Satz 6.3 und Satz 6.4 ergibt sich:

Satz 8.4. *Jedes konvexe Mittelpunktspolytop ist als Schnitt durch den Schwerpunkt eines höherdimensionalen regulären Simplex und als senkrechte Parallelprojektion eines höherdimensionalen regulären Simplex darstellbar.*

Satz 8.3 und Satz 8.4 lassen sich leicht durch Angabe der entsprechenden Abschätzungen ergänzen.

Literatur

[1] Bonnesen, T., u. W. Fenchel: Theorie der konvexen Körper. Berlin 1934. — [2] Schoute, P. H.: Mehrdimensionale Geometrie, Bd. II. Leipzig 1905.

Schwelm (Westf.), Tannenstr. 8

(Eingegangen am 22. November 1955)

Landsberg, M.
Math. Zeitschr. Bd. 65, S. 104—112 (1956)

Lineare topologische Räume, die nicht lokalkonvex sind

Von
Max Landsberg

Einleitung und Ergebnisse

Bekanntlich sind für die Funktionalanalysis die lokalkonvexen Räume von fundamentaler Bedeutung. In den beiden letzten Jahrzehnten hat man jedoch auch spezielle lineare topologische Räume, die nicht lokalkonvex sind, näher untersucht (s. z. B. M. M. Day [2], S. S. Walters [9]). Der Nachweis, daß es sich hierbei um nicht lokalkonvexe Räume handelt, war nicht in allen Fällen einfach. So behandelte S. S. Walters eingehend die Räume H^r für $0<r<1$ ([9], [10]), konnte aber seine Vermutung, daß diese Räume nicht lokalkonvex sind, nicht beweisen (s. [10]). Die Richtigkeit der Annahme von Walters wies A. E. Livingston [4] nach.

Die vorliegende Note enthält unter anderem ein einfaches Kriterium, mit dem sich in vielen Fällen die Tatsache, daß ein vorliegender linearer topologischer Raum nicht lokalkonvex ist, leicht feststellen läßt.

Der Ausgangspunkt für die hier durchgeführten Überlegungen ist die folgende Definition. Eine Teilmenge M eines linearen Raumes soll r-konvex $(0<r\leq 1)$ heißen, wenn aus $a\geq 0$, $b\geq 0$, $a^r+b^r=1$, $x\in M$, $y\in M$ stets $ax+by\in M$ folgt. Wir bezeichnen einen linearen topologischen Raum als r-konvex, wenn jede Nullumgebung eine r-konvexe Nullumgebung enthält. Offensichtlich ist die Klasse der 1-konvexen Räume mit der Gesamtheit der lokalkonvexen Räume identisch. Die meisten linearen topologischen Räume, die bisher zu funktionalanalytisch interessanten Aussagen Anlaß gaben, sind für ein gewisses r $(0<r\leq 1)$ r-konvex.

Man erkennt leicht, daß jeder r-konvexe Raum auch s-konvex ist für jedes s mit $0<s<r$. Dagegen ist ein r-konvexer Raum mit $0<r<1$ im allgemeinen nicht s-konvex für $r<s\leq 1$. Bezüglich dieser Bemerkung gilt nun der folgende Sachverhalt: *Es sei E ein linearer topologischer Raum und φ ein im Nullelement von E stetiges Funktional (auf E). Außerdem existiere ein r mit $0<r<1$ und eine beschränkte Folge (v_n) aus E, so daß für jedes natürliche n und für beliebige positive Zahlen $\varrho_1, \ldots, \varrho_n$*

$$\varphi(\varrho_1 v_1+\cdots+\varrho_n v_n)\geq \varrho_1^r+\cdots+\varrho_n^r$$

ist. Dann ist E nicht s-konvex für $r<s\leq 1$, insbesondere also nicht lokalkonvex.

An verschiedenen Beispielen soll die Anwendbarkeit dieses Kriteriums dargelegt werden. Im Anschluß an [4], [9] und [10] behandeln wir zunächst einen relativ einfachen Fall. Es sei $0<r<1$ und G ein linearer Funktionenraum, dessen Elemente komplexwertige Funktionen sind, die im Innern des

Einheitskreises der komplexen z-Ebene definiert und dort stetig sind. Insbesondere gehöre zu G jede Funktion, die für $|z|<1$ mit einem Polynom $a_0+a_1z+\cdots+a_mz^m$ übereinstimmt. Alle $f\in G$ mit

$$q(f)=\sup_{t\in(0,1)}\int_0^{2\pi}|f(te^{i\vartheta})|^r\,d\vartheta<+\infty$$

bilden dann einen linearen Funktionenraum $H^r(G)$, den die Metrik $q(f-g)$ $(f, g\in H^r(G))$ zu einem linearen topologischen Raum macht. Es wird gezeigt, daß $H^r(G)$ für kein s mit $r<s\leqq 1$ s-konvex sein kann.

Im nächsten Fall sei F ein linearer Folgenraum, der alle finiten Folgen enthalten soll, und (p_n) eine Folge von reellen Zahlen mit $0<p_n\leqq 1$ $(n=1, 2, \ldots)$, $0<\liminf_{n\to\infty} p_n<1$. Alle $x=(a_n)$ aus F mit

$$p(x)=\sum_{n=1}^{\infty}|a_n|^{p_n}<+\infty$$

bilden dann einen linearen Folgenraum $l(F;(p_n))$, der durch die Metrik $p(x-y)$ $(x, y\in l(F;(p_n)))$ zu einem linearen topologischen Raum wird. Es zeigt sich, daß $l(F;(p_n))$ r-konvex für jedes r mit $0<r<\liminf_{n\to\infty} p_n$ ist, aber für kein s mit $\liminf_{n\to\infty} p_n<s\leqq 1$ s-konvex sein kann.

Für $F=\omega$, wo ω der Raum aller Folgen ist, findet man einige Angaben über $l(\omega;(p_n))=l((p_n))$ bei H. Nakano [6].

Für $F=\omega$ und $p_n=r$ $(0<r<1; n=1, 2, \ldots)$ haben wir es mit dem Raum l_r zu tun. Daß l_r nicht lokalkonvex ist, ist bekannt (s. z.B. Mazur-Orlicz [5], A. Tychonoff [8] $(r=1/2)$). Man kann l_r noch unter einem anderen Gesichtspunkt betrachten. Es sei Z die Menge aller natürlichen Zahlen, S_0 der σ-Ring aller Teilmengen von Z und μ_0 dasjenige Maß auf S_0, das durch $\mu_0(\{n\})=1$ $(n=1, 2, \ldots)$ bestimmt ist. Dann ist l_r mit dem zu Z, S_0, μ_0 gehörigen Raum L_r identisch und für jedes $f\in L_r$ ist

$$\int|f|^r\,d\mu_0=\sum_{n=1}^{\infty}|f(n)|^r.$$

Im Spezialfall Z, S_0, μ_0 ist also L_r $(0<r<1)$ für kein s mit $r<s\leqq 1$ s-konvex. Daß in gewissen Sonderfällen L_r $(0<r<1)$ nicht lokalkonvex ist, ist bekannt (s. z.B. M. M. Day [2], Mazur-Orlicz [5]). Ist allgemeiner S ein σ-Ring auf einer Menge E und μ ein Maß auf S, so wird man fragen, unter welchen weiteren Bedingungen für E, S, μ die zugehörigen Räume L_r $(0<r<1)$ nicht s-konvex für $r<s\leqq 1$ sind. Mit Hilfe des oben angeführten Satzes ergibt sich:

1. E sei ein lokalkompakter Raum mit unendlich vielen Elementen, der σ-Ring S enthalte das System K_0 aller kompakten Teilmengen von E, die ein G_δ sind. Für jedes $A\in K_0$, das einen inneren Punkt besitzt, sei $\mu(A)$ endlich und positiv. Dann ist L_r $(0<r<1)$ für kein s mit $r<s\leqq 1$ s-konvex.

2. E sei eine unendliche (bezüglich S, μ) meßbare Gruppe. Auch dann kann L_r $(0<r<1)$ für kein $s\in(r, 1]$ s-konvex sein.

Im zweiten Fall, wo keine Topologie auf E gegeben ist, erscheint es zunächst problematisch, ob man das oben angegebene Kriterium anwenden kann. Die Einführung der WEILschen Topologie, durch die E zu einer topologischen Gruppe mit einer lokalkompakten vollständigen Hülle wird, beseitigt jedoch jede Schwierigkeit.

Lineare topologische Räume, die r-konvex sind

Wir betrachten nur lineare Räume, die komplex sind. Der Begriff Topologie ist im Sinne von BOURBAKI (N. BOURBAKI [1]) zu verstehen, jedoch soll (im Gegensatz zu BOURBAKI) ein topologischer Raum immer ein HAUSDORFF-Raum sein.

In einem linearen Raum wollen wir eine Teilmenge als absolut r-konvex bezeichnen, wenn sie r-konvex (s. Einleitung) ist und mit x auch immer $e^{i\varrho}x$ (ϱ reell) enthält.

Bemerkung 1. *Der lineare topologische Raum E sei r-konvex und U eine Nullumgebung. Dann enthält U eine Nullumgebung, die offen und absolut r-konvex ist.*

Beweis. U enthält eine abgeschlossene und r-konvexe Nullumgebung V. V wiederum enthält eine Nullumgebung W, zu der mit x stets auch $e^{i\varrho}x$ (ϱ reell) gehört. Die r-konvexe Hülle von W, d.h. die kleinste W enthaltende r-konvexe Teilmenge von E, sei W_0. Berücksichtigt man $W_0 \subset V \subset U$, $\overline{W}_0$ ist die abgeschlossene Hülle von W_0, so sieht man, daß das Innere von $\overline{W}_0$ eine offene und absolut r-konvexe Nullumgebung ist, die ganz in U liegt.

Ein Funktional auf dem linearen Raum E ist eine Abbildung von E in die Menge der reellen Zahlen. Das Funktional φ wird als positiv-homogen bzw. als subadditiv bezeichnet, wenn $\varphi(tx) = t\varphi(x)$ $(x \in E,\ t > 0)$ bzw. $\varphi(x+y) \leq \varphi(x) + \varphi(y)$ $(x, y \in E)$ ist. Das Funktional φ heiße eine r-Halbnorm, wenn φ subadditiv und $\varphi(ax) = |a|^r \varphi(x)$ $(x \in E,\ a$ komplex) ist. Ist außerdem $\varphi(x) \neq 0$ für jedes vom Nullelement verschiedene x aus E, so sprechen wir von einer r-Norm.

Bemerkung 2. *E sei ein linearer topologischer Raum und U eine offene und absolut r-konvexe Nullumgebung. Dann existiert genau eine r-Halbnorm φ auf E mit*

$$U = \{x \in E : \varphi(x) < 1\}.$$

Beweis. In naheliegender Weise setzen wir

$$\varphi(x) = \inf\{\varrho^r : \varrho > 0 \quad \text{und} \quad (1/\varrho)\, x \in U\}.$$

Mit einfacher Rechnung bestätigt man $\varphi(ax) = |a|^r \varphi(x)$ $(x \in E,\ a$ komplex) und $U = \{x \in E : \varphi(x) < 1\}$. Weiter gibt es zu jedem $x \in E$ bzw. $y \in E$ ein $\varrho > 0$ bzw. $\sigma > 0$ mit $(1/\varrho)\, x \in U$ bzw. $(1/\sigma)\, y \in U$. Dann gehört auch

$$\frac{\varrho}{(\varrho^r + \sigma^r)^{1/r}} \cdot \frac{1}{\varrho}\, x + \frac{\sigma}{(\varrho^r + \sigma^r)^{1/r}} \cdot \frac{1}{\sigma}\, y = \frac{1}{(\varrho^r + \sigma^r)^{1/r}}\, (x + y)$$

zur (r-konvexen) Menge U. Also ist $q(x+y) < \varrho^r + \sigma^r$ z. B. auch für $\varrho = (\varphi(x) + 1/n)^{1/r}$, $\sigma = (q(y) + 1/n)^{1/r}$ bei beliebigem natürlichem n. Hieraus folgt unmittelbar die Subadditivität von q. Die Eindeutigkeitsaussage ergibt sich sofort aus dem folgenden Hilfssatz, dessen Beweis wir uns schenken können.

Hilfssatz 1. *q und ψ seien zwei positiv-homogene Funktionale auf dem linearen Raum E. Außerdem sei $q(x) \geq 0$ $(x \in E)$ und aus $q(x) < 1$ folge stets $\psi(x) < 1$. Dann ist $\psi(x) \leq q(x)$ für alle x aus E.*

Bemerkung 3. *In einem linearen Raum sei M eine r-konvexe Teilmenge, die mit x auch immer ϱx $(0 < \varrho < 1)$ enthält. Dann ist M auch s-konvex für $0 < s < r$.*

Beweis. Es sei $0 < s < r$, $a \geq 0$, $b \geq 0$, $a^s + b^s = 1$, $x \in M$, $y \in M$. Dann gehört auch

$$y_0 = (a/q)\, x + (b/q)\, y$$

zu M für $q = (a^r + b^r)^{1/r}$. Denn es ist $(a/q)^r + (b/q)^r = 1$. Nun ist

$$q^s = (a^r + b^r)^{s/r} \leq a^s + b^s = 1,$$

also $q \leq 1$. Nach Voraussetzung gehört damit auch $q\, y_0 = a\, x + b\, y$ zu M, M ist s-konvex.

Aus dieser Bemerkung folgt sofort

Satz 1. *E sei ein r-konvexer Raum. Dann ist E auch s-konvex für jedes s mit $0 < s < r$. Insbesondere ist also jeder lokalkonvexe Raum auch s-konvex für $0 < s < 1$.*

Wir erinnern daran, daß in einem linearen topologischen Raum eine Teilmenge A als beschränkt bezeichnet wird, wenn es zu jeder Nullumgebung U ein gewisses $\varrho > 0$ mit $A < \varrho U$ gibt.

Satz 2. *E sei ein linearer topologischer Raum, φ ein im Nullelement von E stetiges Funktional. Außerdem existiere eine beschränkte Folge (v_n) aus E und ein r mit $0 < r < 1$, so daß für jede natürliche Zahl n und für beliebige positive Zahlen $\varrho_1, \ldots, \varrho_n$ stets*

$$\varphi(\varrho_1 v_1 + \cdots + \varrho_n v_n) \geq \varrho_1^r + \cdots + \varrho_n^r$$

ist. Dann kann E nicht s-konvex für $r < s \leq 1$ sein. Insbesondere ist E nicht lokalkonvex.

Beweis. E sei doch s-konvex für ein gewisses s mit $r < s \leq 1$. Nun ist $U = \{x \in E : \varphi(x) < 1 + \varphi(o)\}$ eine Umgebung vom Nullelement o des Raumes E. Nach Bemerkung 1 enthält U eine Nullumgebung V, die offen und absolut s-konvex ist. Die mit V nach Bemerkung 2 assoziierte s-Halbnorm sei Φ. Nach Voraussetzung existiert ein $k > 0$, so daß $\Phi(v_n) \leq k$ für alle n ist. Es sei

$$w_n = v_1 + (1/2^{1/r})\, v_2 + \cdots + (1/n^{1/r})\, v_n \qquad (n = 1, 2, \ldots).$$

Dann ist

$$\begin{aligned} \Phi(w_n) &\leq \Phi(v_1) + (1/2^{s/r})\, \Phi(v_2) + \cdots + (1/n^{s/r})\, \Phi(v_n) \\ &\leq k\,(1 + 1/2^{s/r} + \cdots + 1/n^{s/r}), \end{aligned}$$

also $\Phi(w_n) < k\,\zeta\left(\frac{s}{r}\right)$ für jedes n. Das Element

$$w_n' = \left(\frac{1}{k\,\zeta\left(\frac{s}{r}\right)}\right)^{1/s} w_n$$

gehört somit für jedes n zu V, also auch zu U. Das ist aber nicht möglich, da wegen

$$\varphi(w_n') \geqq \left(\frac{1}{k\,\zeta\left(\frac{s}{r}\right)}\right)^{r/s} (1 + 1/2 + \cdots + 1/n)$$

nicht für jedes n $\varphi(w_n') < 1 + \varphi(o)$ sein kann.

Die Räume $H^r(G)$ $(0 < r < 1)$

Satz 3. *$H^r(G)$ $(0 < r < 1$; s. Einleitung$)$ ist nicht s-konvex für $r < s \leqq 1$. Insbesondere ist also $H^r(G)$ nicht lokalkonvex.*

Beweis (vgl. A. E. LIVINGSTON [4]). C sei der lineare Raum aller auf $0 \leqq \vartheta \leqq 2\pi$ erklärten und dort stetigen komplexwertigen Funktionen. Die Norm $\|h\| = \sup_{\vartheta \in [0, 2\pi]} |h(\vartheta)|$ $(h \in C)$ macht C zu einem BANACH-Raum, durch

$$\hat{q}(h) = \int_0^{2\pi} |h(\vartheta)|^r \, d\vartheta$$

ist auf C eine wegen

(1) $$\hat{q}(h) \leqq 2\pi \|h\|^r \qquad (h \in C)$$

stetige r-Norm (s. Einleitung) gegeben. Zu jedem natürlichen n gibt es ein $h_n \in C$ mit $\hat{q}(h_n) = 2$, das auf den Intervallen $\left[0, 2\pi \frac{n}{n+1}\right]$, $\left[2\pi \frac{n+1}{n+2}, 2\pi\right]$ verschwindet. Offensichtlich gilt dann für jedes n und für beliebige komplexe Zahlen $a_1, \ldots, a_n$

(2) $$\hat{q}(a_1 h_1 + \cdots + a_n h_n) = 2(|a_1|^r + \cdots + |a_n|^r).$$

Weiter existiert nach einem bekannten Satz zu jedem h_n ein trigonometrisches Polynom

$$t_n(\vartheta) = \sum_{k=-s_n}^{s_n} a_{k\,n}\, e^{i k \vartheta}$$

mit

(3) $$\|t_n - h_n\| \leqq \left(\frac{1}{2\pi}\right)^{1/r}.$$

Mit Hilfe von t_n bilden wir das Polynom

$$P_n(z) = \sum_{k=-s_n}^{s_n} a_{k\,n}\, z^{k+s_n},$$

dessen Einschränkung auf $|z| < 1$ mit π_n bezeichnet werden soll. Nach Voraussetzung gehört π_n zu G (s. Einleitung) und daher auch zu $H^r(G)$. Berücksichtigt man (1), (3) und einen bekannten funktionentheoretischen Satz

(PÓLYA-SZEGÖ [7], S. 144), so findet man für jedes n

$$q(\pi_n) = \sup_{t\in(0,1)} \int_0^{2\pi} |P_n(t\,e^{i\vartheta})|^r\,d\vartheta = \lim_{t\to 1} \int_0^{2\pi} |P_n(t\,e^{i\vartheta})|^r\,d\vartheta$$
$$= \hat{q}(t_n) \leqq 2\pi\|t_n - h_n\|^r + \hat{q}(h_n) \leqq 3.$$

Die Folge (π_n) ist also beschränkt im Raum $H^r(G)$. Wir zeigen noch, daß für jedes n und für beliebige positive Zahlen $\varrho_1, \ldots, \varrho_n$

$$q(\varrho_1\pi_1 + \cdots + \varrho_n\pi_n) \geqq \varrho_1^r + \cdots + \varrho_n^r$$

ist, womit nach Satz 2 alles bewiesen ist. Setzen wir $g_n(\vartheta) = e^{i s_n \vartheta}$ $(n = 1, 2, \ldots;$ $0 \leqq \vartheta \leqq 2\pi)$, so ist mit Berücksichtigung von (1), (2), (3)

$$q(\varrho_1\pi_1 + \cdots + \varrho_n\pi_n) = \hat{q}\left(\sum_{j=1}^{n} \varrho_j g_j t_j\right)$$
$$\geqq \hat{q}\left(\sum_{j=1}^{n} \varrho_j g_j h_j\right) - \hat{q}\left(\sum_{j=1}^{n} \varrho_j g_j (t_j - h_j)\right)$$
$$\geqq 2\sum_{j=1}^{n} \varrho_j^r - 2\pi \sum_{j=1}^{n} \varrho_j^r \|t_j - h_j\|^r$$
$$\geqq \sum_{j=1}^{n} \varrho_j^r.$$

Die Räume $l(F;(p_n))$

Im Anschluß an die in der Einleitung angegebenen Bezeichnungen setzen wir noch $\lambda = \liminf_{n\to\infty} p_n$.

Satz 4. *$l(F;(p_n))$ ist r-konvex für jedes r mit $0 < r < \lambda$.*

Beweis. Es sei r eine Zahl aus $(0, \lambda)$. Es gibt dann eine natürliche Zahl n_0 mit $p_n \geqq r$ für alle $n > n_0$. Für $x = (a_n)$ aus $l(F;(p_n))$ sei

$$\hat{p}(x) = |a_1|^r + \cdots + |a_{n_0}|^r + \sum_{n=n_0+1}^{\infty} |a_n|^{p_n}.$$

$\hat{p}$ ist ein subadditives Funktional auf $l(F;(p_n))$, für das insbesondere $\hat{p}(a\,x) \leqq |a|^r \hat{p}(x)$ (a komplex, $|a| \leqq 1$, $x \in l(F;(p_n))$) gilt. Für jedes natürliche m sei $U_m = \{x \in l(F;(p_n)) : \hat{p}(x) \leqq 1/m\}$. Die U_m bilden eine Basis des Filters aller Nullumgebungen. Wir zeigen noch, daß jedes U_m r-konvex ist. Es sei $a, b \geqq 0$ und $a^r + b^r = 1$. Für zwei beliebige Elemente x, y aus U_m ist dann

$$\hat{p}(a\,x + b\,y) \leqq a^r \hat{p}(x) + b^r \hat{p}(y) \leqq (a^r + b^r) \cdot \frac{1}{m} = \frac{1}{m}.$$

Also gehört auch $a\,x + b\,y$ zu U_m.

Satz 5. *$l(F;(p_n))$ ist nicht s-konvex für $\lambda < s \leqq 1$. Insbesondere ist $l(F;(p_n))$ nicht lokalkonvex.*

Beweis. s gehöre zum Intervall $(\lambda, 1]$. Es wird ein $\varkappa$ mit $\lambda < \varkappa < s$ gewählt. Es gibt dann eine Teilfolge (p_{n_j}) von (p_n) mit $p_{n_j} \leq \varkappa$ $(j = 1, 2, \ldots)$. Für jedes $x = (a_n)$ aus $l(F; (p_n))$ ist

$$\tilde{p}(x) = \sum_{j=1}^{\infty} |a_{n_j}|^{\varkappa}$$

endlich, $\tilde{p}$ ist offensichtlich eine $\varkappa$-Halbnorm auf $l(F; (p_n))$. Die Zahlenfolge, die an n_j-ter Stelle eine 1, sonst aber nur Nullen hat, bezeichnen wir mit v_j. Die v_j gehören nach Voraussetzung (s. Einleitung) zu F, also auch zu $l(F; (p_n))$. Die Folge (v_j) ist in $l(F; (p_n))$ beschränkt, für jedes n und für beliebige positive Zahlen $\varrho_1, \ldots, \varrho_n$ ist

$$\tilde{p}(\varrho_1 v_1 + \cdots + \varrho_n v_n) = \varrho_1^{\varkappa} + \cdots + \varrho_n^{\varkappa}.$$

Nach Satz 2 ist alles bewiesen, d.h. $l(F; (p_n))$ kann nicht s-konvex sein, wenn noch die Stetigkeit von $\tilde{p}$ im Nullelement von $l(F; (p_n))$ gezeigt wird. Hierzu genügt der Nachweis, daß $U = \{x \in l(F; (p_n)) : \tilde{p}(x) \leq 1\}$ eine Nullumgebung ist. Es sei nun U die Nullumgebung, die aus allen $x \in l(F; (p_n))$ mit $p(x) \leq 1$ besteht. Für jedes $x = (a_n)$ aus U ist

$$\tilde{p}(x) \leq \sum_{j=1}^{\infty} |a_{n_j}|^{p_{n_j}} \leq p(x) \leq 1.$$

Also ist $V \supset U$, V ist ebenfalls eine Nullumgebung.

Die Räume $L_r (0 < r < 1)$

Mit kompakt ist bikompakt gemeint. Ist S ein σ-Ring (s. z. B. HALMOS [3]) von Teilmengen einer Menge E mit $\cup \{A : A \in S\} = E$, so soll S ein σ-Ring auf E genannt werden. Ist f eine reellwertige Funktion auf der Menge E, S ein σ-Ring auf E, so heißt f meßbar (HALMOS [3]), wenn für jedes reelle ϱ die Menge $\{x \in E : f(x) \neq 0 \text{ und } f(x) < \varrho\}$ zu S gehört. Damit ist auch klar, was die Meßbarkeit einer komplexwertigen Funktion bedeutet. Bei dieser Definition sind insbesondere diejenigen auf E erklärten charakteristischen Funktionen φ_A meßbar, bei denen $A = \{x \in E : \varphi(x) = 1\}$ zu S gehört, d.h. meßbar ist. Ist E ein topologischer Raum, so sei Σ_0 der kleinste σ-Ring auf E, der alle kompakten Teilmengen von E, die ein G_δ sind, enthält. Die Mengen von Σ_0 sind die BAIREschen Mengen von E.

Es sei nun S ein σ-Ring auf einer Menge E, μ ein Maß auf S, Λ_r $(0 < r < 1)$ der lineare Funktionenraum aller komplexwertigen meßbaren Funktionen f auf E mit integrierbarem $|f|^r$. Alle $f \in \Lambda_r$ mit $\int |f|^r d\mu = 0$ bilden einen Teilraum N_r von Λ_r. Die „Quasimetrik"

$$d(f, g) = \int |f - g|^r d\mu \qquad (f, g \in \Lambda_r)$$

definiert in bekannter Weise auf dem Quotientenraum $L_r = \Lambda_r / N_r$ eine Metrik, durch die L_r zu einem linearen topologischen Raum wird.

Satz 6. *E sei ein lokalkompakter Raum mit unendlich vielen Elementen. S sei ein σ-Ring auf E, der den σ-Ring Σ_0 aller* BAIREschen *Mengen enthält.*

μ sei ein Maß auf S, für jede kompakte Bairesche *Menge A, die einen inneren Punkt besitzt, sei $\mu(A)$ endlich und positiv. Dann ist L_r $(0<r<1)$ für kein s mit $r<s\leq 1$ s-konvex.*

Beweis. Mit $\emptyset$ wird die leere Menge bezeichnet. Es existiert, wie eine einfache Überlegung zeigt, eine Folge (y_n) von Elementen von E und eine Folge (W_n) von Teilmengen von E, so daß W_n Umgebung von y_n und $W_m \cap W_n = \emptyset$ $(m \neq n)$ ist. Jedes W_n enthält eine Umgebung V_n von y_n, die ein kompaktes G_δ ist (Halmos [3], S. 218). Weiter existiert zu jedem n eine stetige Abbildung f_n von E in $[0, 1]$ mit $f_n(y_n)=1$, $f_n(x)=0$ $(x \notin V_n)$. f_n ist meßbar (sogar bezüglich Σ_0; Halmos [3], S. 220), wegen $\mu(V_n)<+\infty$ ist $|f_n|^r$ integrierbar, wegen $\mu(V_n)>0$ ist auch

$$J_n = \int |f_n|^r \, d\mu$$

positiv. Wir setzen $g_n = (1/J_n)^{1/r} f_n$ $(n=1, 2, \ldots)$. Gehört f zu Λ_r, so sei $[f]$ das zugehörige Element in $L_r = \Lambda_r / N_r$. Die $[g_n]$ bilden in L_r eine beschränkte Folge, durch $\psi([f]) = \int |f|^r d\mu$ $(f \in \Lambda_r)$ ist auf L_r eine stetige r-Norm definiert, für jedes n und für beliebige positive Zahlen $\varrho_1, \ldots, \varrho_n$ ist

$$\psi(\varrho_1 [g_1] + \cdots + \varrho_n [g_n]) = \varrho_1^r + \cdots + \varrho_n^r .$$

Nach Satz 2 ist damit die Behauptung bewiesen.

Im folgenden sei E eine Gruppe mit dem Einselement e_0, S wiederum ein σ-Ring auf E, μ ein σ-finites Maß auf S. Alle $A \times B$ $(A, B \in S)$ bilden einen σ-Ring $S \times S$ auf $E \times E$, T sei die durch $(x, y) \to (x, xy)$ erklärte Abbildung von $E \times E$ in sich. Ist A eine Teilmenge von E, so sei A' das Komplement von A in E. Für zwei Teilmengen A, B von E wird $A \Delta B = (A \cap B') \cup (A' \cap B)$ gesetzt (Halmos [3]). E wird als meßbare Gruppe bezeichnet, wenn folgendes gilt: S und μ sind linksinvariant $(xA \in S, \mu(xA) = \mu(A)$ für alle $x \in E, A \in S)$, die Abbildung T führt die (bezüglich $S \times S$) meßbaren Teilmengen von $E \times E$ wieder in meßbare Mengen über, zu jedem von e_0 verschiedenen $x \in E$ existiert ein $A \in S$ mit $0<\mu(A)<+\infty$, $\mu((xA) \Delta A) > 0$.

Satz 7. *Die meßbare Gruppe E besitze unendlich viele Elemente. Dann ist L_r $(0<r<1)$ für kein s mit $r<s\leq 1$ s-konvex. Insbesondere ist L_r nicht lokalkonvex.*

Beweis. Für $A \in S$, $0<\mu(A)<+\infty$, $0<\varepsilon<2\mu(A)$ sei

$$U(A; \varepsilon) = \{x \in E : \mu((xA) \Delta A) < \varepsilon\}.$$

Es gibt dann genau eine Topologie T_0 auf E, bei der E zu einer topologischen Gruppe wird und die $U(A; \varepsilon)$ eine Basis für den Filter aller Umgebungen von e_0 bilden. T_0 ist die sog. Weilsche Topologie von E (Halmos [3], S. 273). Es existiert dann eine lokalkompakte Gruppe $\hat{E}$, so daß E isomorph zu einer Untergruppe $\tilde{E}$ von $\hat{E}$ ist, die in $\hat{E}$ überall dicht liegt. Für die folgenden Überlegungen kann man $\tilde{E} = E$ annehmen. Wir bezeichnen eine Teilmenge A

von E als präkompakt (vgl. BOURBAKI [1], S. 161), wenn in $\hat{E}$ die abgeschlossene Hülle von A kompakt ist; versehen mit der WEILschen Topologie ist also E eine lokal präkompakte Gruppe.

Die Topologie von $\hat{E}$, die auf E die WEILsche Topologie T_0 erzeugt, nennen wir $\hat{T}_0$. Ist A eine Teilmenge von E, so soll die abgeschlossene Hülle von A in E bzw. in $\hat{E}$ mit $\bar{A}$ bzw. mit A^* bezeichnet werden. Es gibt nun (s. Beweis von Satz 6) eine Folge (y_n) von Elementen aus E und eine Folge (W_n) von Teilmengen von E, so daß W_n T_0-Umgebung von y_n, $W_m \cap W_n = \emptyset$ $(m \neq n)$ und $\overline{W}_n = W_n$ ist. W_n^* ist dann eine $\hat{T}_0$-Umgebung von y_n und enthält eine $\hat{T}_0$-Umgebung V_n von y_n, die (in $\hat{E}$) ein kompaktes G_δ ist. Da $\hat{E}$ vollständig regulär ist, existiert zu jedem n eine stetige Abbildung φ_n von $\hat{E}$ in $[0, 1]$ mit $\varphi_n(y_n) = 1$, $\varphi_n(x) = 0$ $(x \in \hat{E},\ x \notin V_n)$. Alle Teilmengen A von $\hat{E}$ mit $A \cap E \in S$ bilden einen σ-Ring $\hat{S}$ auf $\hat{E}$, der die BAIREschen Mengen von $\hat{E}$ enthält (HALMOS [3], S. 276). Insbesondere gehören also alle V_n zu $\hat{S}$, für jedes n ist daher $V_n \cap E$ meßbar in E. Nach einer oben gemachten Bemerkung (s. Beweis von Satz 6) ist φ_n meßbar (bezüglich $\hat{S}$). f_n sei die Einschränkung von φ_n auf E. Dann ist f_n meßbar bezüglich S und $f_n(x) = 0$ $(x \in E,\ x \notin V_n \cap E)$. Wegen $0 < \mu(V_n \cap E) < +\infty$ (HALMOS [3], S. 274) ist $|f_n|^r$ integrierbar und $\int |f_n|^r d\mu > 0$. Nun ist $V_n \cap E \subset W_n^* \cap E = \overline{W}_n = W_n$, also $(V_m \cap E) \cap (V_n \cap E) = \emptyset$ für $m \neq n$. Der Rest des Beweises verläuft wie bei Satz 6.

Literatur

[1] BOURBAKI, N.: Topologie générale, Chap. I—II. Actual. Sci. Industr. 858—1142 (1951). — [2] DAY, M. M.: The spaces L^p with $0 < p < 1$. Bull. Amer. Math. Soc. **46**, 816—832 (1940). — [3] HALMOS, P. R.: Measure Theory. New York 1950. — [4] LIVINGSTON, A. E.: The space H^p, $0 < p < 1$, is not normable. Pacific J. Math. **3**, 613—616 (1953). — [5] MAZUR, S., et W. ORLICZ: Sur les espaces métriques linéaires. I. Studia Math. **10**, 184—208 (1948). — [6] NAKANO, H.: Concave modulars. J. Math. Soc. Japan **5**, 29—49 (1953). — [7] PÓLYA, G., u. G. SZEGÖ: Aufgaben und Lehrsätze aus der Analysis. I. Berlin 1925. — [8] TYCHONOFF, A.: Ein Fixpunktsatz. Math. Ann. **111**, 767—776 (1935). — [9] WALTERS, S. S.: The space H^p with $0 < p < 1$. Proc. Amer. Math. Soc. **1**, 800—805 (1950). — [10] WALTERS, S. S.: Remarks on the space H^p. Pacific J. Math. **1**, 455—471 (1951).

Dresden, Mathematisches Institut der Technischen Hochschule

(Eingegangen am 3. Januar 1956)

Randwertprobleme der Mikrowellenphysik

Von **Fritz E. Borgnis** und **Charles H. Papas**, California Institute of Technology, Pasadena/USA. Mit 75 Textabbildungen. XV, 266 Seiten Gr.-8°. 1955.

Ganzleinen DM 48.—

Inhaltsübersicht: 1. Das elektromagnetische Feld. Allgemeine und spezielle Beziehungen. — 2. Die skalare Greensche Funktion. — 3. Beugung einer ebenen Welle am metallischen Kreiszylinder. Formulierung einer Integralgleichung für den Strombelag und Betrachtungen über deren Lösung. — 4. Formulierung einer stationären Darstellung des Streuquerschnitts für eine ebene Welle, deren elektrisches Feld parallel zur Achse des beugenden Kreiszylinders liegt. — 5. Der Streuquerschnitt bei der Beugung am metallischen Kreiszylinder für eine ebene Welle, deren elektrisches Feld senkrecht zur Zylinderachse liegt. — 6. Eine stationäre Darstellung für das Fernfeld bei der Beugung einer ebenen Welle am Kreiszylinder. — 7. Wahl einer Näherungsfunktion für den Strombelag am Kreiszylinder. — 8. Berechnung der Streuquerschnitte bei der Beugung am Kreiszylinder. — 9. Der Streuquerschnitt bei der Beugung einer ebenen Welle an einem unendlich langen metallischen Streifen und am unendlich langen Spalt. — 10. Die offen abstrahlende koaxiale Leitung mit Schirm. — 11. Unstetiger Übergang zwischen zwei koaxialen kreiszylindrischen Leitungen. — 12. Die kapazitive Blende im rechteckigen Hohlleiter. — 13. Die induktive Blende im rechteckigen Hohlleiter. — 14. Näherungsweise Bestimmung der Grenzfrequenz von zylindrischen Hohlleitern beliebigen Querschnitts. — 15. Näherungsweise Bestimmung der Eigenfrequenzen von Hohlraumresonatoren beliebiger Gestalt. — 16. Die Weitwinkel-Konusantenne. — 17. Die zylindrische Antenne. — 18. Anhang: A. Zum Zusammenhang zwischen der stationären Darstellung nach Schwinger und Rayleighs Resultat für das Fernfeld bei der Beugung einer skalaren Welle an einer kleinen Scheibe. — B. Zur Beziehung zwischen Transmissionsfaktor und Fernfeld beim ebenen Schirm und deren Verwendung zur experimentellen Ermittlung des Transmissionsfaktors. — C. Grundzüge der Dyadenrechnung (Dyadenalgebra). — D. Die dyadische Greensche Funktion. — Namen- und Sachverzeichnis.

SPRINGER-VERLAG / BERLIN · GÖTTINGEN · HEIDELBERG

Landolt-Börnstein, Zahlenwerte und Funktionen aus Physik, Chemie, Astronomie, Geophysik und Technik

Sechste Auflage der „Physikalisch-chemischen Tabellen". Unter vorbereitender Mitwirkung von J. D'Ans, A. Eucken †, G. Joos, W. A. Roth † herausgegeben von **J. Bartels, P. ten Bruggencate, K. H. Hellwege, Kl. Schäfer, E. Schmidt.** In vier Bänden.

Soeben erschien:

II. Band: **Eigenschaften der Materie in ihren Aggregatzuständen**

3. Teil: **Schmelzgleichgewichte und Grenzflächenerscheinungen**

Bearbeitet von E. Beger, K. Bratzler, A. Dietzel, J. L. v. Eichborn, W. Eitel, G. G. Grau, A. Kofler, Kl. Schäfer, H. Scholze, J. Stauff, R. Vogel, A. Wacker, G. Weitzel. Herausgegeben von **Klaus Schäfer** und **Ellen Lax.** Mit 998 Abbildungen. XI, 535 Seiten 4°. 1956. In Moleskin DM 198.—

Inhaltsübersicht: **Schmelzgleichgewichte.** Schmelzgleichgewichte von Metall-Legierungen. — Schmelzgleichgewichte binärer und ternärer Systeme anorganischer Verbindungen und reziproker Salzpaare mit Ausnahme silikatischer Verbindungen. — Schmelzgleichgewichte silikatischer Systeme. — Schmelzgleichgewichte in organischen Systemen. — Schmelzgleichgewichte in anorganisch-organischen Systemen. — **Charakteristische Konstanten für das Gleichgewicht an Phasengrenzflächen: Grenzflächenspannung (Grenzflächentension).** Allgemeines. — Grenzflächenspannung reiner Flüssigkeiten gegen ihren Dampf oder Luft (Oberflächenspannung) und Parachor. — Grenzflächenspannung von Lösungen gegen Luft. — Grenzflächenspannung zweier nichtmischbarer Flüssigkeiten. — Randwinkel an fest-flüssigen Grenzflächen. — Grenzflächenfilme auf Wasser. — **Adsorption.** Adsorption aus der Gasphase. — Adsorption aus flüssiger Phase an pulverförmigen Adsorptionsmitteln. — **Chromatographie (Papier-Chromatographie).**

Die weiteren Teile des II. Bandes werden behandeln:

1. Teil: **Mechanisch-thermische Konstanten homogener Systeme. — Mechanisch-thermische Zustandsgrößen.**
2. Teil: **Gleichgewichte außer Schmelzgleichgewichten.**
4. Teil: **Kalorische Zustandsgrößen.**
5. Teil: **Physikalische und chemische Kinetik und Akustik.**
6. Teil: **Elektrische Eigenschaften; Optische Konstanten (1. Teil).**
7. Teil: **Optische Konstanten (2. Teil); Magnetische Eigenschaften.**

SPRINGER-VERLAG / BERLIN · GÖTTINGEN · HEIDELBERG

Diesem Heft liegen zwei Prospekte des Springer-Verlages, Berlin - Göttingen - Heidelberg, bei Springer-Verlag, Berlin · Göttingen · Heidelberg. — Druck der Universitätsdruckerei H. Stürtz AG., Würzburg
Printed in Germany